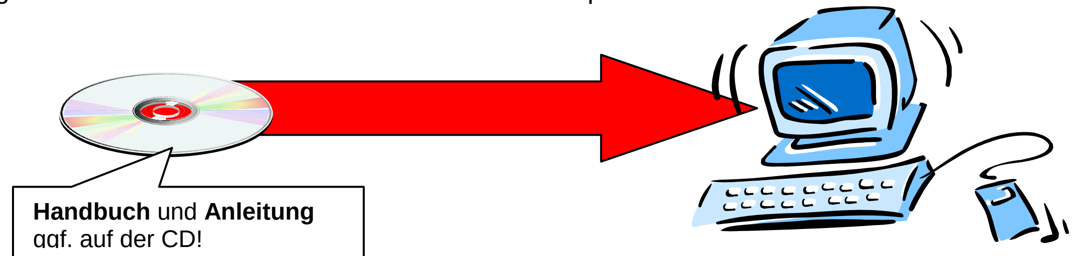


DAKOTA SUPPORT-GUIDE

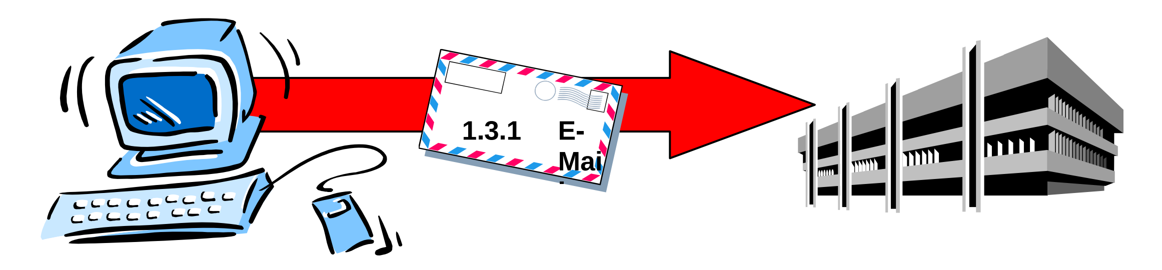
1 Allgemeine Fragen

1.1 *Was ist zu tun?*

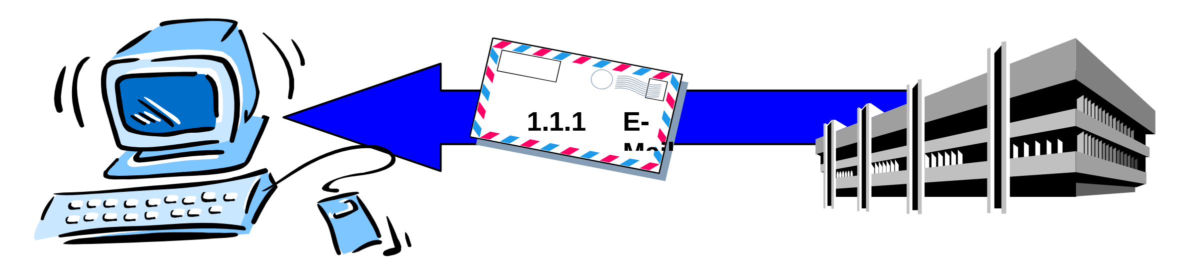
1. Schritt - Installation
Legen Sie die dakota-CD in das Laufwerk Ihres Computer und starten Sie die Installation



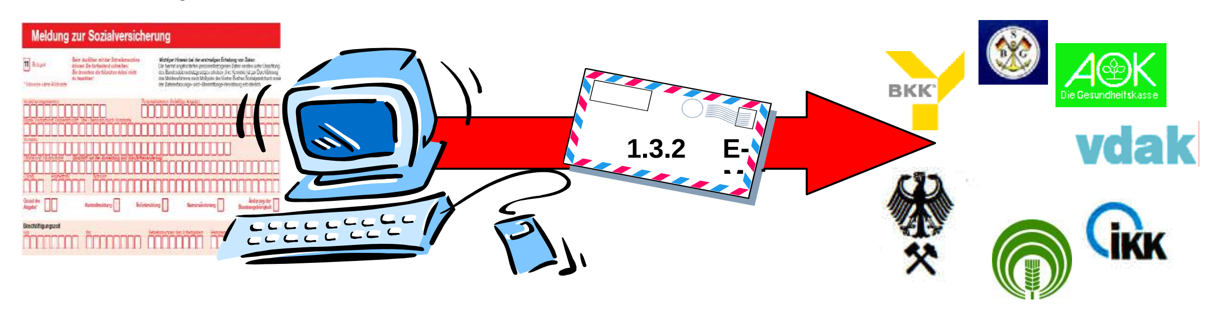
2. Schritt - E-Mail-Konfiguration und Zertifikat beantragen
Nutzen Sie bereits E-Mail - prima, dakota beantragt Ihr Zertifikat bequem per E-Mail.



3. Schritt - Zertifikat und Stammdaten einlesen
Nach ca. 1 Woche erhalten Sie Ihr Zertifikat vom TrustCenter per E-Mail. Mit einem Doppelklick auf die Anhänge lesen Sie die Stammdaten mit dakota ein.



4. Schritt - Beitragsnachweise und Sozialversicherungsmeldungen per E-Mail versenden
Jetzt können Sie mit dakota alle Meldungen und Beiträge per **E-Mail an alle Krankenkassen** versenden **- Papier ist ‚out'**.



1.2 *Wie lange dauert es, bis ich meine Antwort vom TrustCenter erhalte?*

Sobald Sie die schriftlichen Antragsunterlagen beim ITSG TrustCenter (per Fax ODER Postweg) einsenden und diese erfasst wurden, erhalten Sie von uns eine Auftragsnummer per E-Mail.
Die Erfassung Ihrer Papierunterlagen kann je nach Aufkommen bis zu 10 Tagen in Anspruch nehmen.

Nach Erhalt Ihrer Auftragsnummer können Sie den Stand Ihres Antrages jederzeit im Internet unter http://trustcenter.itsg.de im Bereich Online Auftragsverfolgung einsehen.

Falls Ihre Antragsunterlagen unvollständig oder fehlerhaft sind, können Sie dies in der Auftragsverfolgung einsehen.

Für eine Zertifizierung im ITSG TrustCenter benötigen wir

- den unterschriebenen schriftlichen Zertifizierungsantrag
- den Ausdruck des öffentlichen Schlüssels mit persönlicher Unterschrift (dies entfällt für dakota-Kunden ab der Version 2.5, wenn über Punkt 1 (Antragsteller) der Hashcode steht)
- die Kopien zur Identitätsfeststellung des Ansprechpartners (z. B. Personalausweis, siehe Antrag)

und im Verfahren für sonstige Leistungserbringer zusätzlich:
- die Kopien zur Bestätigung der IK-Nummer (siehe Antrag)

Senden Sie Ihre Unterlagen an folgende Adresse:
ITSG TrustCenter
Postfach 12 30
49702 Meppen
oder
per Fax: 05931-848840

1.3 *Wie erfahre ich, ob mein Antrag vollständig ist?*

Ein vollständiger Zertifizierungsantrag besteht aus den folgenden Teilen:

Elektronische Zertifizierungsanfrage
Der Dateiname Ihrer elektronischen Anfrage trägt Ihre Betriebsnummer / IK-Nummer und die Endung .CRQ (z. B. 12345678.crq).
Wenn Sie diese Datei an unsere E-Mail-Adresse

Itsg-crq@atosorigin.com

senden, erhalten Sie von uns eine Quittung per E-Mail.

Papierantrag
Bitte stellen Sie sicher, dass Sie den zweiseitigen Antrag vollständig (jede Frage beantwortet) ausgefüllt und unterschrieben per Brief oder per Fax an uns gesendet haben.

Identifikation des verantwortlichen Ansprechpartners
Kopieren Sie bitte den Personalausweis, den Führerschein oder den Reisepass des verantwortlichen Ansprechpartners.

Im Verfahren der sonstigen Leistungserbringer muss eine Kopie zur Bestätigung der IK-Nummer beigefügt werden.

Sobald Sie die schriftlichen Antragsunterlagen beim ITSG TrustCenter (per Fax ODER Postweg) einsenden und diese erfasst wurden, erhalten Sie von uns eine Auftragsnummer per E-Mail.
Die Erfassung Ihrer Papierunterlagen kann je nach Aufkommen bis zu 10 Tagen in Anspruch nehmen.

Nach Erhalt Ihrer Auftragsnummer können Sie den Stand Ihres Antrages jederzeit im Internet unter http://trustcenter.itsg.de im Bereich Online Auftragsverfolgung einsehen.

Senden Sie Ihre Unterlagen an folgende Adresse:
ITSG TrustCenter
Postfach 12 30
49702 Meppen
oder
per Fax: 05931-848840

Bitte erzeugen Sie während der Bearbeitung der Zertifizierungsanfrage keinen neuen Schlüssel in Ihrem Softwareprodukt. Ihre bereits gestellte Zertifizierung wird ansonsten ungültig und Sie benötigen ein neues Zertifikat, wodurch Ihnen weitere Kosten entstehen.

Falls Ihre Antragsunterlagen unvollständig oder fehlerhaft sind, können Sie dies in der Auftragsverfolgung einsehen.
„Wie lange dauert es, bis ich meine Antwort vom TrustCenter erhalte?“

1.4 *Wozu gibt es eigentlich ein TrustCenter?*

Ein TrustCenter erstellt digitale Zertifikate (Schlüssel) für den gesicherten Datenaustausch im Gesundheitswesen und stellt die öffentlichen Schlüssel bereit. Weitere Infos finden Sie unter http://trustcenter.itsg.de .

Es ist erforderlich, dass alle öffentlichen Schlüssel der Teilnehmer in einem zentralen Verzeichnis publiziert werden. Jeder Benutzer kann darauf zugreifen und die öffentlichen Schlüssel zur Prüfung der Unterschriften heranziehen. Zudem muss sichergestellt werden, dass die Zuordnung einer elektronischen Unterschrift zu einer natürlichen Person von einer vertrauenswürdigen Instanz geprüft und erst danach der Schlüssel für die öffentliche Nutzung bereitgestellt wird.
Diese Instanz bildet das TrustCenter. Jeder Teilnehmer muss einen Antrag auf Zertifizierung an das TrustCenter richten. In einer Registrierungsstelle werden die Angaben des Antragsstellers geprüft und danach die Erstellung eines Zertifikates freigegeben. Danach signiert das TrustCenter den öffentlichen Schlüssel des Teilnehmers mit einem eigenen Zertifikat und stellt den jeweiligen öffentlichen Schlüssel in das öffentliche Schlüsselverzeichnis.
Die Art der Identifikation kann unterschiedlich sein und reicht in der Praxis von der einfachen Identifikation per E-Mail bis zur Vorlage z. B. eines Personalausweises oder eines Reisepasses. Dabei dürfte klar sein, dass die Identifikation mittels E-Mail nur einen relativ geringen Wert hat, da insoweit Täuschungen über die wahre Identität relativ einfach zu bewerkstelligen sind.

1.5 Was ist ein Zertifikat?

Das Zertifikat wird für die Verschlüsselung benötigt. Vereinfacht ausgedrückt ist es der von einem TrustCenter bestätigte öffentliche Schlüssel eines jeden Teilnehmers im Datenaustauschverfahren. Das Zertifikat hat eine begrenzte Gültigkeitsdauer von 3 Jahren und kann danach nicht mehr weiter verwendet werden.
Nach Ablauf des Zertifikates muss eine Neuzertifizierung erfolgen.

1.5 *Wie fülle ich den Antrag richtig aus?*

Ausfüllhilfe zum Zertifizierungsantrag

Wählen Sie bitte zuerst das Verfahren, für das Sie sich in unserem TrustCenter anmelden möchten. Nehmen Sie am Leistungserbringerverfahren teil, geben Sie bitte Ihr **Institutionskennzeichen** (**IK)** an. Nehmen Sie am Arbeitgeberverfahren teil, geben Sie bitte Ihre **Betriebsnummer (BN)** an.

Antragsteller

An dieser Stelle sind die erforderlichen Angaben zum Antragsteller zu machen. Durch diese Angaben wird der Teilnehmer gegenüber dem TrustCenter identifiziert. Name des Antragstellers (Firma / Institution), IK- oder Betriebsnummer und verantwortlicher Ansprechpartner (alle mit * gekennzeichneten Felder) werden in das Zertifikat übernommen und sollen mit den Eingaben in die verwendete Software bei der Generierung des Schlüsselpaares übereinstimmen.
Der Teilnehmer sollte unbedingt darauf achten, dass alle Angaben korrekt sind.
Widersprüche zwischen den Angaben auf dem Antragsformular und der Eingabe in die Software können dazu führen, dass der Teilnehmer Korrekturen durchführen muss. Insbesondere müssen alle Angaben in den mit * gekennzeichneten Feldern unbedingt korrekt sein, da sie in elektronischen Verzeichnissen veröffentlicht werden und den Kommunikationspartnern u. a. zum Auffinden des Zertifikates für einen Teilnehmer dienen.

Beispiel:

Name des Antragstellers* (Firma / Institution):	Physiotherapie Erwin Mueller
IK-Nummer / Betriebsnummer:	**IK123123123 / BN12312312**
verantwortlicher Ansprechpartner:	**Erwin Mueller**

Sie können bei der Eingabe in die Software Groß- und Kleinbuchstaben verwenden: A - Z, die Ziffern 0 - 9 und **nur** die Sonderzeichen: Schrägstrich, Leerschritt, Minus und Punkt und ( ).
Verwenden Sie bitte bei der Eingabe keine anderen Sonderzeichen, auf **keinen** Fall: Umlaute, ß, +, &, Semikolon, Unterstrich, Komma , \, Anführungszeichen, § etc., da wir sonst aus technischen Gründen die Datei *.crq nicht maschinell verarbeiten können.

Änderungen des Namens, der IK- oder Betriebsnummer bzw. des verantwortlichen Ansprechpartners nach Erteilung des Zertifikates bedingen die Ausstellung eines neuen Zertifikates!
Verantwortlicher Ansprechpartner kann nur eine natürliche Person und nicht etwa eine Abteilung sein. Als verantwortlicher Ansprechpartner ist die Person zu benennen, die für den sicheren Umgang mit dem privaten Schlüssel verantwortlich ist. Sie sollte durch Vor- und Zuname identifiziert werden.
Sollten Antragsteller und verantwortlicher Ansprechpartner **nicht** identisch sein, benötigt der Ansprechpartner eine Vollmacht des Antragstellers für das Verfahren. Aufgrund dieser Vollmacht kann das TrustCenter dann sicher sein, dass der verantwortliche Ansprechpartner im Namen des Antragsteller tätig wird.
Geben Sie bitte Ihre korrekte E-Mail-Adresse an.

Sie haben dann die Möglichkeit, das Zertifikat des TrustCenters in Form der Datei 12345678.crp und die aktuell gültige öffentliche Schlüsselliste der Datenannahmestellen der GKV (z. B. Datei ANNAHME.KEY) nach der Zertifizierung einmalig per E-Mail zu erhalten. Kreuzen Sie hierfür „Zertifizierungsantwort an diese E-Mail-Adresse“ an.

Sollten Sie die Zertifizierungsantwort auf Diskette wünschen, kreuzen Sie bitte diese Option an. Entnehmen Sie die Bearbeitungs- und Versandpauschalen für Disketten unserer aktuell gültigen Preisliste oder dem Internet unter http://trustcenter.itsg.de.
Die ITSG bietet verschiedene E-Mail-Services (z. B. für die automatische Zusendung der öffentliche Schlüsselliste der Datenannahmestellen der GKV, bei Änderungen der Liste oder für die Zusendung von allgemeinen TrustCenter-Informationen) an. Sie können sich hierzu im Internet auf der Seite **http://trustcenter.itsg.de** anmelden.
Die Gültigkeitsdauer des Zertifikates ist im Datenaustauschverfahren für alle Teilnehmer auf 3 Jahre festgelegt.

Identifikation des verantwortlichen Ansprechpartners
Kreuzen Sie hier an, welches der aufgeführten Dokumente Sie in Kopie dem Zertifizierungsantrag als Anlage beifügen.
Im Leistungserbringerverfahren kopieren Sie bitte zusätzlich

- den Vergabebescheid für IK-Nummern der Sammel- und Verteilungsstelle IK (SVI) der Arbeitsgemeinschaft Institutionskennzeichen (IK) oder ein vergleichbares Dokument über die Zulassung als Leistungserbringer

Fügen Sie diese Kopie(n) Ihrem Antrag bei.

Angaben zur eingesetzten Software
Damit sich das TrustCenter im Falle möglicher Rückfragen bzgl. der eingesetzten Software an das entsprechende Softwarehaus direkt wenden kann, bitten wir Sie an dieser Stelle um den Namen Ihres Softwarelieferanten und der eingesetzten Fachanwendung.

Schlüsselgenerierung
Die vom Antragsteller für die Generierung des Schlüssels eingesetzte Software erstellt eine Datei in der die wesentlichen Angaben des vom TrustCenter später zu erstellenden Zertifikates bereits enthalten sind. Deshalb wird von der Software neben den Angaben zum Antragsteller (s. o.) auch die Angabe des Namens des TrustCenters verlangt (soweit dieser nicht voreingestellt ist). Auch hier ist aus technischen Gründen unbedingt auf eine korrekte Schreibweise zu achten. Evtl. fehlerhafte Voreinstellungen in der Software sind zu korrigieren.

Für das **PEM** Verfahren nutzen Sie bitte die folgenden TrustCenter:

Der Name des TrustCenters für den Datenaustausch im Gesundheitswesen ist:

ITSG TrustCenter fuer den Datenaustausch mit Leistungserbringern

Der Name des TrustCenters für den Datenaustausch im Arbeitgeberverfahren ist:

ITSG TrustCenter fuer das Arbeitgeberverfahren

Für das **PKCS#7** Verfahren nutzen Sie bitte die folgenden TrustCenter:

Der Name des TrustCenters für den Datenaustausch im Gesundheitswesen ist:

ITSG TrustCenter fuer sonstige Leistungserbringer

Der Name des TrustCenters für den Datenaustausch im Arbeitgeberverfahren ist:

ITSG TrustCenter fuer Arbeitgeber

Die Datei mit den wesentlichen Angaben des vom TrustCenter später zu erstellenden Zertifikates wird vom Teilnehmer direkt an das TrustCenter übermittelt. Der Dateiname hat das Format: 12312312.crq. Die Ziffern geben die IK- bzw. Betriebsnummer wieder, wobei die neunte Stelle der IK-Nummer (Prüfziffer) weggelassen wird.
Der Teilnehmer sollte angeben, wie die Datei an das TrustCenter übermittelt wird. Dadurch wird dem TrustCenter die Zuordnung zum Zertifizierungsantrag erleichtert. Das TrustCenter wird Ihnen mit Hilfe des gleichen Dienstes die Zertifizierungsantwort (Datei im Format *.crp) zukommen lassen.
Bei evtl. aufkommenden Fragen zur Schlüsselgenerierung wird der Lieferant der Software dem Antragsteller sicherlich gern behilflich sein.

Kundenkennwort
Bei telefonischen Anfragen bzgl. des Antrages kann es notwendig sein, dass der Antragsteller das Kundenkennwort angibt, um sich zu legitimieren, bevor er eine Auskunft vom TrustCenter erhält. Von besonderer Bedeutung ist es, im Falle einer beantragten Sperrung des Zertifikates, einen möglichen Missbrauch auszuschließen. Von der Legitimation des Teilnehmers muss sich das TrustCenter aber auch dann überzeugen, wenn der Teilnehmer Informationen zu den im TrustCenter über ihn gespeicherten personenbezogenen Daten wünscht.

Sperrung
Falls das TrustCenter auf Grund möglicher Eilbedürftigkeit und Unkenntnis des Kundenkennwortes auf telefonische Anforderung hin auch ohne Angabe des Kundenkennwortes das Zertifikat sperren soll, bitte ankreuzen.

Rechnungsanschrift
Im Regelfall werden Anschrift des Antragstellers und die Rechnungsanschrift identisch sein, sodass keine Angaben zur Rechnungsanschrift erforderlich sind.

Zahlungsweise
Überweisen Sie bitte das Entgelt für die Zertifizierung in Höhe des Rechnungsbetrages sofort und ohne Abzug nach Erhalt der Rechnung auf das Konto der ITSG. Bitte geben Sie bei der Überweisung als Verwendungszweck unbedingt die Rechnungsnummer an. Ohne diese Angabe können Zahlungen u.U. nicht zugeordnet werden.

Bemerkungen / Besonderheiten
Hier wird Raum gegeben, auf besondere Umstände bei der Zertifizierung hinzuweisen. Ein Beispiel könnte sein, dass das Zertifikat erst ab einem bestimmten Datum erstellt werden soll oder dass es sich um einen Folgeantrag handelt o. ä. Hier können Sie alles vermerken, was Ihnen hinsichtlich der Bearbeitung der Zertifizierung wichtig erscheint.

Unterschrift des verantwortlichen Ansprechpartners
Sind Antragsteller und verantwortlicher Ansprechpartner nicht identisch, so benötigt der Ansprechpartner eine Vollmacht des Antragstellers (s. o.). Hier wird davon ausgegangen, dass der Ansprechpartner auch den Zertifizierungsantrag stellen darf. Sofern dies aus organisatorischen Gründen nicht der Fall ist, muss der Ansprechpartner neben dem Antragsteller unterzeichnen.
Der verantwortliche Ansprechpartner wird darauf hingewiesen, dass die Veröffentlichung des Zertifikates in elektronischen Verzeichnissen für das Verfahren zwingend erforderlich ist und dass er im eigenen Interesse den genannten Verpflichtungen nachkommen muss, um mögliche Schäden zu vermeiden.



10 Schritte zum Zertifikat

- ☐ Informieren Sie sich über das Verfahren anhand der dem Zertifikatsantrag beigefügten Darstellungen. Die Erstellung eines Zertifikatsantrages wird durch eine Ausfüllhilfe unterstützt.
- ☐ Erzeugen Sie mit der bei Ihnen installierten Sicherheitssoftware einen eigenen Schlüssel.
- ☐ Erstellen Sie eine Zertifikatsanfrage mit der Sicherheitssoftware. Diese erzeugt eine Datei *.crq und es wird dabei ein Ausdruck eines Komprimates bzw. der Schlüsselausdruck erstellt. Bitte unterschreiben Sie den Schlüsselausdruck und legen Sie ihn als Anlage zum Antrag bei.
- ☐ Legitimieren Sie sich anhand der o. g. Kopie(n) und legen Sie auch diese(s) als Anlage dem Antrag bei.
- ☐ Wenn Sie als Beauftragter handeln, fügen Sie bitte noch eine Vollmacht der Firma bzw. Institution als Anlage bei.
- ☐ Unterschreiben Sie den Zertifizierungsantrag bei Punkt 10. „Unterschrift des verantwortlichen Ansprechpartners".
- ☐ Sie können den Antrag zusammen mit den Anlagen senden
  per Post an: ITSG TrustCenter, Postfach 12 30, 49702 Meppen
  per Fax an: ITSG TrustCenter, 05931-848840
- ☐ Übermitteln Sie den öffentlichen Schlüssel (die Datei in dem Format *.crq) an das ITSG TrustCenter
  per Post zusammen mit den restlichen Unterlagen auf Diskette.
  per E-Mail an: itsg-crq@atosorigin.com
  per FTAM im Leistungserbringerverfahren (IK): 05931/805-553
  per FTAM im Arbeitgeberverfahren (BN): 05931/805-555
  Der geheime Schlüssel verbleibt in Ihrem Besitz und damit auch hinsichtlich der sicheren Aufbewahrung in Ihrer persönlichen Verantwortung.
- ☐ Das TrustCenter führt alle Unterlagen zusammen und prüft den Dateninhalt des elektronischen und des schriftlichen Antrages auf Übereinstimmung. Darüber hinaus werden die Eindeutigkeit und die Länge des Schlüssels geprüft.
  Bei positivem Ergebnis wird Ihr Zertifikat erzeugt und in öffentliche Verzeichnisse eingestellt.
- ☐ Das Zertifikat Ihres öffentlichen Schlüssels (Datei im Format *.crp) können Sie entsprechend Ihrer technischen Möglichkeiten auf folgenden Wegen erhalten und in Ihre Anwendungssoftware integrieren.
  per Diskette zusammen mit einer einmaligen Zusendung der öffentlichen Schlüsselliste der Datenannahmestellen der GKV (Datei annahme.key). Entnehmen Sie bitte die Bearbeitungs- und Versandpauschalen für Disketten unserer aktuell gültigen Preisliste oder dem Internet unter http://trustcenter.itsg.de .
  per E-Mail (wenn auf dem Antrag vermerkt) an Ihre E-Mail-Adresse zusammen mit einer einmaligen Zusendung der öffentlichen Schlüsselliste der Datenannahmestellen der GKV (Datei annahme.key)
  per FTAM im Leistungserbringerverfahren (IK): 05931/805-553
  per FTAM im Arbeitgeberverfahren (BN): 05931/805-555
  per E-Mail-Responder an: itsg-dir@atosorigin.com [send 12345678.crp, send annahme.key]

So erhalten Sie Ihr Zertifikat vom ITSG TrustCenter im Arbeitgeberverfahren

Sie senden uns:

Sie erzeugen mit Ihrem PC

1. eine Schlüsseldatei (*.crq)

entweder per E-Mail:
itsg-crq@atosorigin.com

oder per FTAM:
Datenaustausch Leistungserbringer:
05931 - 805 - 553

Datenaustausch Arbeitgeber:
05931 - 805 - 555

oder Diskette:
per Post (s.u.)

Sie drucken mit Ihrem PC

2. ein Papierantrag (2 Seiten)
(bitte unterschreiben)

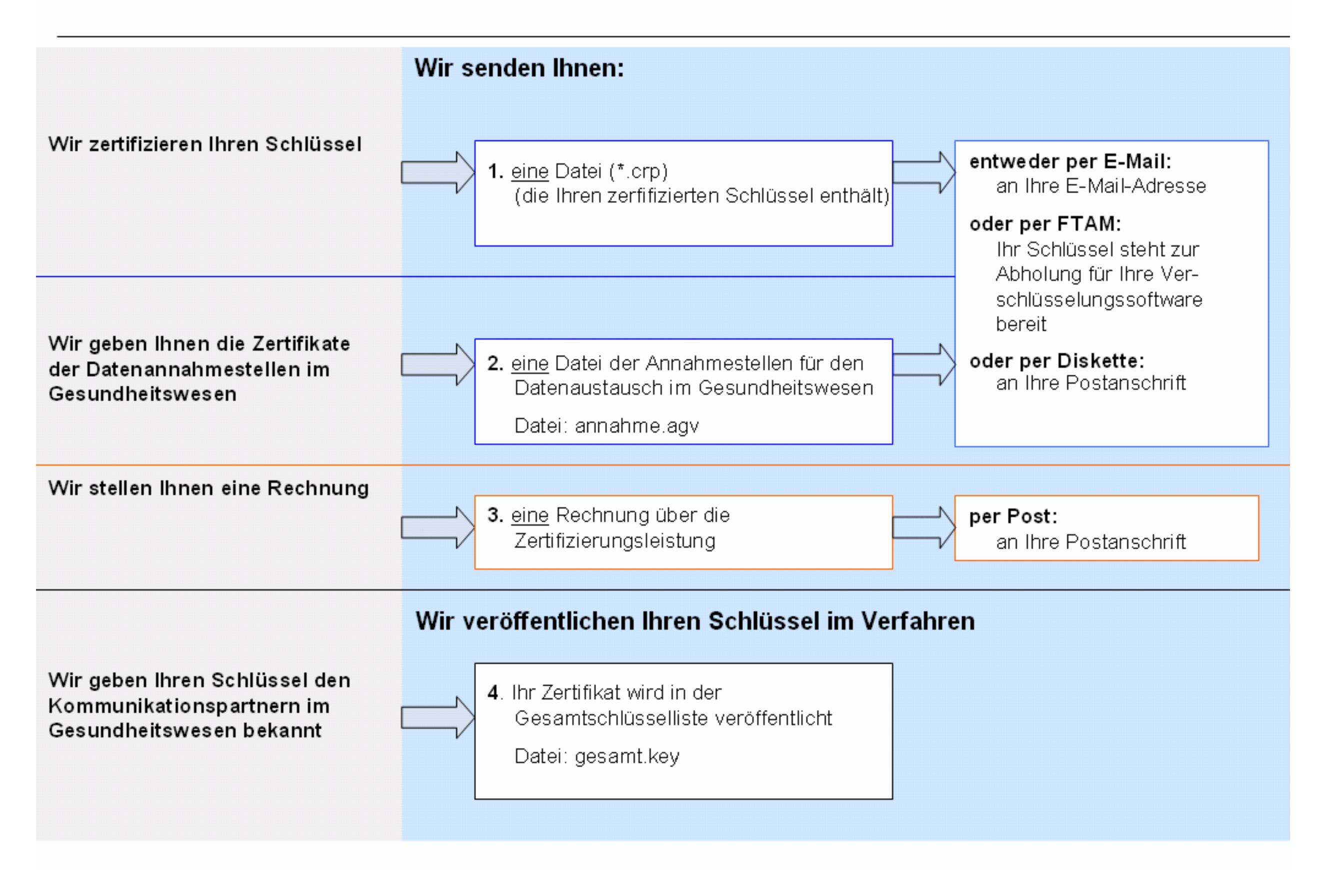
3. einen Schlüsselausdruck
(Zahlen- und Buchstabenkombinationen, bitte unterschreiben)

Sie erstellen

4. eine Kopie Ihres Personalausweis

per FAX:
05931 / 848840 **oder**

per Post:
ITSG TrustCenter
Postfach 1230
49702 Meppen



1.6 *Was kostet ein Zertifikat beim ITSG TrustCenter?*

Der aktuelle Preis für ein Zertifikat des ITSG-TrustCenters und die AGB´s können Sie unter http://trustcenter.itsg.de einsehen.

(Stand: Dezember 2005)
Die Bearbeitungsgebühr für ein Zertifikat des ITSG-TrustCenters beträgt zur Zeit im Rahmen einer befristeten Sonderaktion bis zum 31.12.2005 einmalig 45,00 € (zzgl. MwSt.) für eine Gültigkeitsdauer von 3 Jahren ab Ausstellungsdatum.

Alle Angaben sind ohne Gewähr und Änderungen sind vorbehalten. Den aktuellen Zertifikatspreis finden Sie stets auf http://trustcenter.itsg.de .

1.7 *Wo kann ich Informationen über den elektronischen Datenaustausch mit Krankenkassen finden?*

Die rechtlichen und technischen Vorgaben für die Übermittlung elektronischer Daten an die Krankenkassen finden Sie unter http://www.gkv-ag.de und http://www.datenaustausch.de.

Die gesetzliche Grundlage für die elektronische Übermittlung von Sozialversicherungsmeldungen zum 01.01.2006 für Arbeitgeber erhalten Sie hier: http://www.gkv-ag.de/aktuelles/dateien/Aktuelles_2005-05.pdf

1.8 *Wann ändern sich die elektronischen Schlüssel der Annahmestellen?*

Die Annahmestellen der gesetzlichen Krankenkassen erstellen alle 3 Jahre einen neuen Schlüssel. Die Schlüssel der Annahmestellen laufen stichtagsbezogen zum 31.12. aus.

Dadurch ist eine Aktualisierung der öffentlichen Schlüsseldatei nur einmal alle 3 Jahre am Jahresanfang notwendig.

Nächster Schlüsselwechsel: **31.12.2007**

Um die aktuellen Schlüssel der Annahmestellen für das Arbeitgeberverfahren zu erhalten:
http://www.itsg.de/tc/tc/tc-ftp/tc-download/sv.agv.asp

Um die aktuellen Schlüssel der Annahmestellen für das Leistungserbringerverfahren zu erhalten:
http://www.itsg.de/tc/tc/tc-ftp/tc-download/sv.lev.asp

Die ITSG bietet ebenfalls einen Update-Service an. Sollten sich die Schlüssel der Annahmestellen im Gesundheitswesen ändern, erhalten Sie automatisch eine E-Mail:
http://www.itsg.de/tc/service/updateservice.asp

1.9 *Ich bin Arbeitgeber mit mehreren Betriebsnummern oder ich bin Steuerberater mit mehreren Mandanten. Welche Betriebsnummer muss ich für die Zertifizierung angeben?*

Bei Abrechnung von mehreren Betriebsnummern erstellen Sie NUR für die Betriebsnummer des Abrechnungsbetriebes (Für diesen Betrieb ist auch die Zulassung zur DEÜV erfolgt!) einen Schlüssel und versenden damit die kompletten Daten.
Es genügt lediglich ein Zertifikat für Sie als "Versendende-Stelle" zu beantragen.

Bei der Verschlüsselung handelt es sich um eine Transportsicherung, die keine Aussagen über den Inhalt trifft. Bitte erstellen Sie NUR für Ihre Betriebsnummer ein Zertifikat und senden Sie alle Meldungen Ihrer Mandanten mit Ihrem Zertifikat.
dakota ist somit mandantenfähig und Sie benötigen nur EIN Zertifikat.
Es genügt lediglich ein Zertifikat für Sie als "Versendende-Stelle" zu beantragen.

1.10 *Wie kann ich den TrustCenter-Antrag noch einmal ausdrucken?*

Um ein Zertifikat beim TrustCenter zu erhalten, müssen Sie den elektronischen Antrag am Bildschirm ausfüllen und zusammen mit dem Fingerabdruck des privaten Schlüssels ausdrucken. Wenn hier Probleme mit dem Drucker auftreten, können Sie den Antrag an dieser Stelle erneut drucken. Dazu rufen Sie den TrustCenter-Antrag auf und wählen Sie den Knopf **>Antrag drucken<** oder **>Neuversand<** aus.



1.11 *Wie finde ich die Betriebsnummern der Krankenkassen?*

Eine komplette Information über alle Betriebsnummern der Krankenkassen finden Sie unter http://www.gkv-ag.de. Dort können Sie auch unter **>Grundlagen<** eine Datei herunterladen.

1.12 *Wie verarbeite ich die E-Mail vom TrustCenter mit meinem Zertifikat?*

Vom TrustCenter erhalten Sie eine E-Mail mit 3 Anhängen, Ihrem Zertifikat (Betriebsnummer.crp bzw. IK-Nummer.crp), der öffentlichen Schlüsselliste (Annahme.agv bzw. Annahme.key) und einem Zip-Archiv (Betriebsnummer.zip bzw. IK-Nummer.zip). Die beiden erstgenannten Dateien müssen lediglich mit einem Doppelklick ausgeführt werden oder Sie speichern beide Dateianhänge in einem Dateiverzeichnis und verarbeiten die Dateien im dakota-Assistenten.

Sollten Sie Dateien nicht verarbeiten können, entpacken Sie bitte das Zip-Archiv und verwenden Sie die Dateien, wie oben beschrieben.

Sollte Ihr Zip-Archiv auch beschädigt sein, können Sie unter http://trustcenter.itsg.de im Bereich Online Auftragsverfolgung unter Angabe Ihrer Betriebsnummer und Ihrer Auftragsnummer Ihre Schlüsselantwort erneut herunterladen.

1.13 *Wie finde ich die Daten der Annahmestellen, z. B. die E-Mail-Adressen?*

Die Daten der Annahmestellen sind bereits in dakota unter Stammdaten hinterlegt.
Eine Auflistung für das Arbeitgeberverfahren finden Sie hier. Die Ersatzkassen, z. B. Barmer, DAK oder GEK nehmen Ihre Daten über den VdAK an, daher haben diese keine E-Mail Adresse:

BITTE BEACHTEN SIE:
Die Stammdaten in dakota sind vollständig und müssen nicht ergänzt werden.

BN	NAME	EMAIL
15027365	Techniker Krankenkasse	Annahme über VdAK
29137937	Kaufmännische Krankenkasse -	Annahme über VdAK
15031806	Hanseatische Krankenkasse	Annahme über VdAK
31702878	AOK-WL	da@dta.aok.de
42938966	Barmer Ersatzkasse	Annahme über VdAK
66761998	GEK Gmuender Ersatzkasse	Annahme über VdAK
15035218	DAK Deutsche Angestellten-	Annahme über VdAK
20013461	Handelskrankenkasse Bremen	Annahme über VdAK
98094032	Bundesknappschaft	Annahme über VdAK
35382142	BKK - Bundesverband	ag@bkk-bv.de
66667777	Deutsche Rentenversicherung	AlgII@vdr.de
64672791	AOK Baden Württemberg - Die	da@dta.aok.de
01000262	AOK-ISC Teltow	da@dta.aok.de
05174740	AOK Sachsen	da@dta.aok.de
20158137	AOK-Bremen / Bremerhaven	da@dta.aok.de
29720865	AOK-Niedersachsen	da@dta.aok.de
33526082	AOK Westfalen-Lippe - Die	da@dta.aok.de
34364249	AOK Rheinland - Die	da@dta.aok.de
01000251	ARGE AOK	da@dta.aok.de
47860681	ARGE AOK-Rechenzentrum Mitte,	da@dta.aok.de
01000240	DAV Suhl KKS-AG	da@dta.aok.de
55420162	AOK- Die Gesundheitskasse im	da@dta.aok.de
87880235	AOK Bayern - Die	da@dta.aok.de
51605725	ARGE AOK-Rechenzentrum Mitte,	da@dta.aok.de
37912580	IKK-Bundesverband	dav01@b2b.mailorbit.de
47056789	LKK-Bundesverband der	dav01@b2b.mailorbit.de
15451439	VdAK	dav01@b2b.mailorbit.de
98000006	Bundesknappschaft	dav01@b2b.mailorbit.de
99086875	See-Krankenkasse	meldungen.see-kk@see-bg.de

1.14 *Wo erhalte ich Unterstützung für mein dakota-Problem?*

Die ITSG vertreibt dakota ausschließlich an Wiederverkäufer. Wir bitten Sie daher um Verständnis, dass wir Ihnen KEINEN direkten Endkundensupport anbieten können. Unterstützung können Sie von dem Softwaredistributor erhalten, vom dem Sie dakota erworben haben.

Sie finden aber die Antwort auf viele Ihrer Fragen in den folgenden FAQ´s oder im Benutzerhandbuch von dakota. Das Benutzerhandbuch können Sie hier herunterladen:

http://www.itsg.de/dakotaag/dakota_forum/dateien/Dakota%20Benutzer%20HandbuchV3.0.PDF

2 Technisch orientierte Fragen

2.1 *Welche E-Mail-Systeme kann ich mit dakota verwenden?*

Es liegen positive Meldungen vor, dass die folgenden E-Mail-Programme problemlos eingesetzt werden können. Eine Garantie kann dafür aber nicht übernommen werden!

dakota bietet Ihnen, wie bereits im Handbuch beschrieben, mehrere Möglichkeiten sich am E-Mail-System anzubinden:

SMTP
MAPI
Verzeichnisausgabe

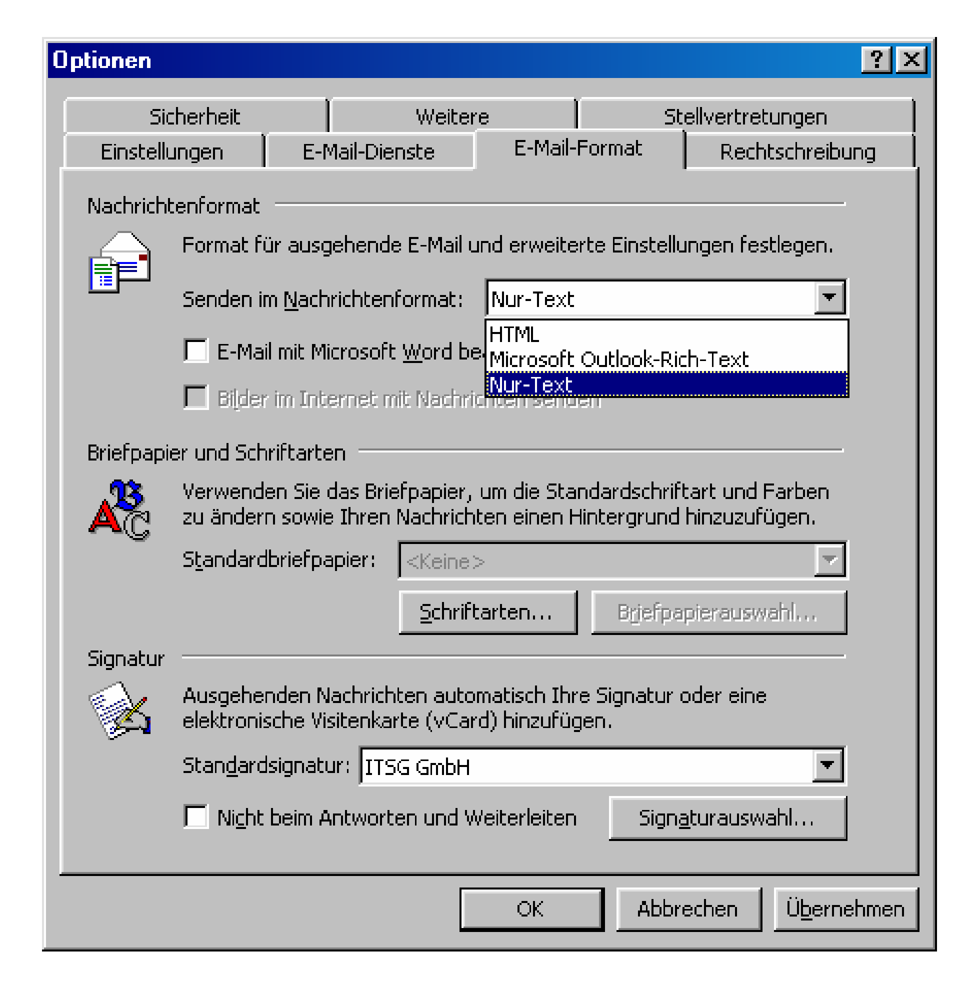
Hier finden Sie das dakota-Handbuch zum Download:
http://www.itsg.de/dakotaag/dakota_forum/dateien/Dakota%20Benutzer%20HandbuchV3.0.PDF

2.2 *Wie stelle ich MS Outlook 2000/XP/2003 für dakota ein?*

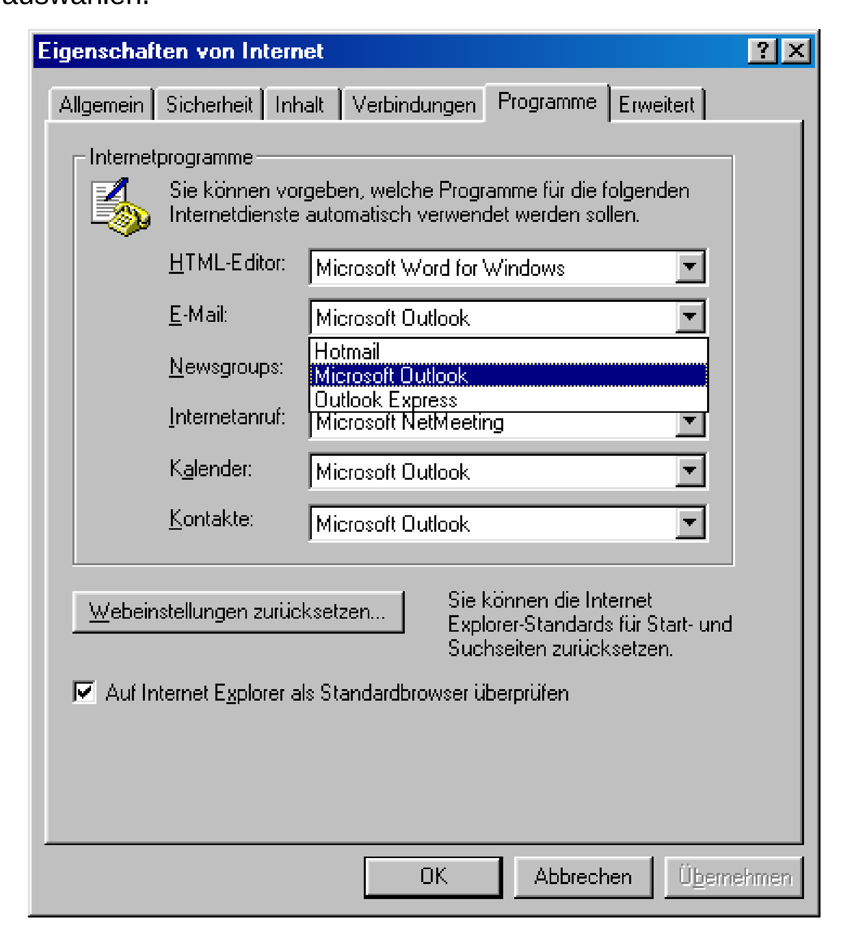
Beim Einsatz von MS Outlook kann es passieren, dass ein eigenes Format von Microsoft die zwei notwendigen Anhänge zusammenfasst und die Annahmestellen diese E-Mails nicht verarbeiten können (MS Rich-Text Format). Der E-Mail-Anhang erhält dann die Endung *.DAT, z. B. winmail.DAT

Dies geschieht, wenn Ihr Microsoft Outlook E-Mail Nachrichten im „Rich-Text“ Format versendet. Bitte ändern Sie Ihr Nachrichtenformat auf „Nur-Text“.
Ein evtl. vorhandener MS Exchange Server darf diese Einstellung nicht verändern.

Stellen Sie unter **Extras / Optionen /** Register **E-Mail-Format** das Nachrichtenformat auf „Nur-Text“ ein.



Stellen Sie MS Outlook als E-Mail-Programm in Ihren Internet-Optionen ein:
Systemsteuerung / Internet-Optionen / Register-Programme als E-Mail: „Microsoft Outlook“ auswählen.



2.3 *Wie richte ich mein E-Mail-Programm mit meinem Provider ein?*

Eine kleine Anleitung, wie mit Outlook Express ein E-Mail-Konto eingerichtet wird, finden Sie im Benutzerhandbuch von dakota. Uns ist es leider nicht möglich, für alle E-Mail-Programme eine solche Anleitung zu geben, aber hier sind einige Links, die Ihnen weiterhelfen können:

Hier finden Sie eine kurze Anleitung für fast alle E-Mail-Programme. Bitte beachten Sie, hier ist ein Bespiel des Providers freenet:
http://www.freenet.de/hilfe/email/emailclients/config/index.html

Hier finden Sie die neueste Version des Internet-Explorers 6 SP1 (mit Outlook Express):
http://www.microsoft.com/downloads/details.aspx?FamilyID=1e1550cb-5e5d-48f5-b02b-20b602228de6&displaylang=de

Ein weiteres Bespiel mit T-Online:

Um mit Outlook Express über den Provider T-Online E-Mail´s versenden zu können, muss zunächst eine DFÜ-Verbindung eingerichtet werden. Es ist leider nicht möglich, die bestehenden Einwahlverbindungen, die das sog. „StartCenter“ schafft, zu nutzen.

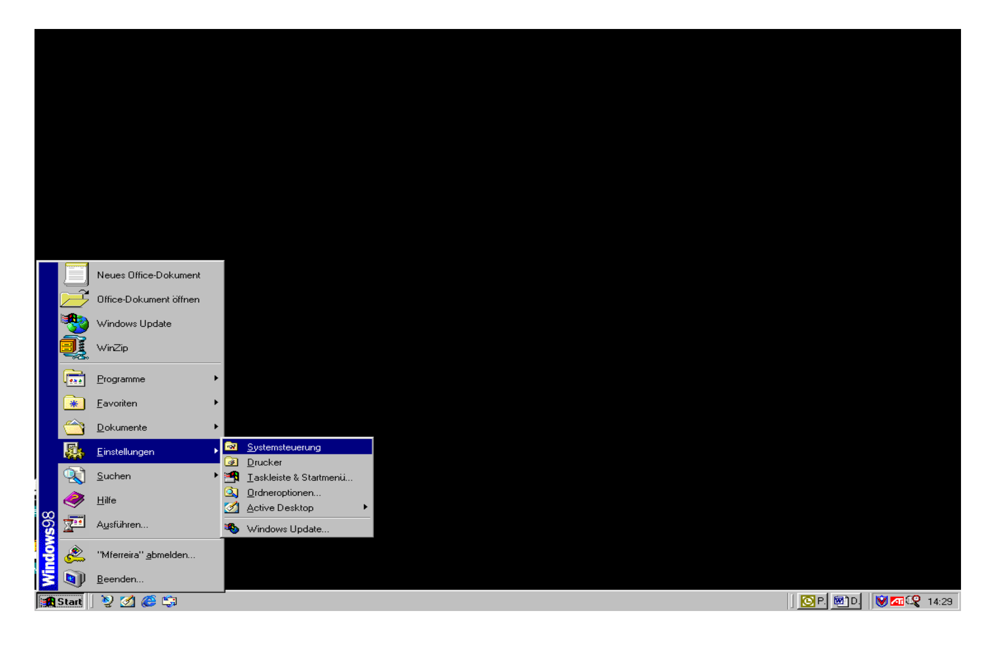
Eine genaue Anleitung finden Sie bei T-Online unter:
http://service.t-online.de/c/17/25/04/1725046.html

Im zweiten Schritt wird das E-Mail-Konto in Outlook Express für den Versand mit T-Online eingerichtet:
http://service.t-online.de/c/16/88/63/1688630.html

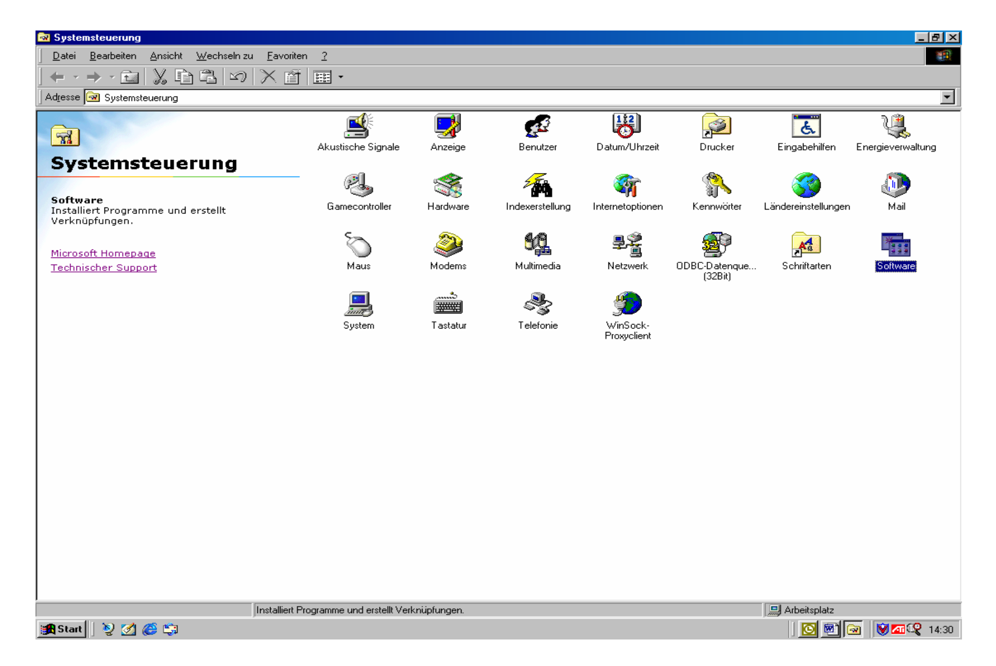
2.4 *Das Versenden mit Outlook 2000/2002/2003 funktioniert nicht?*

Bitte legen Sie sich, bevor Sie mit der Einstellung von Outlook beginnen, die Office-CD bereit.

Schritt 1
Über den Start-Button in **>Einstellungen<** gehen und **>Systemsteuerung<** auswählen.

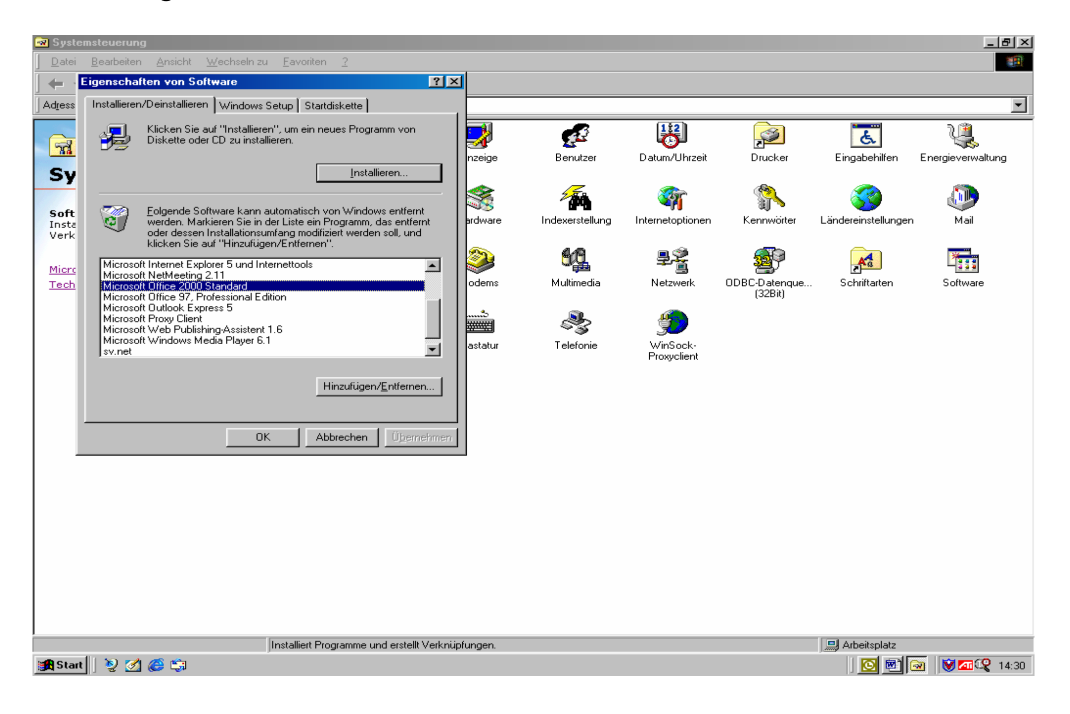


Schritt 2
Sie befinden sich jetzt in dem Fenster **>Systemsteuerung<**. Klicken Sie die Datei **>Software<** doppelt an.



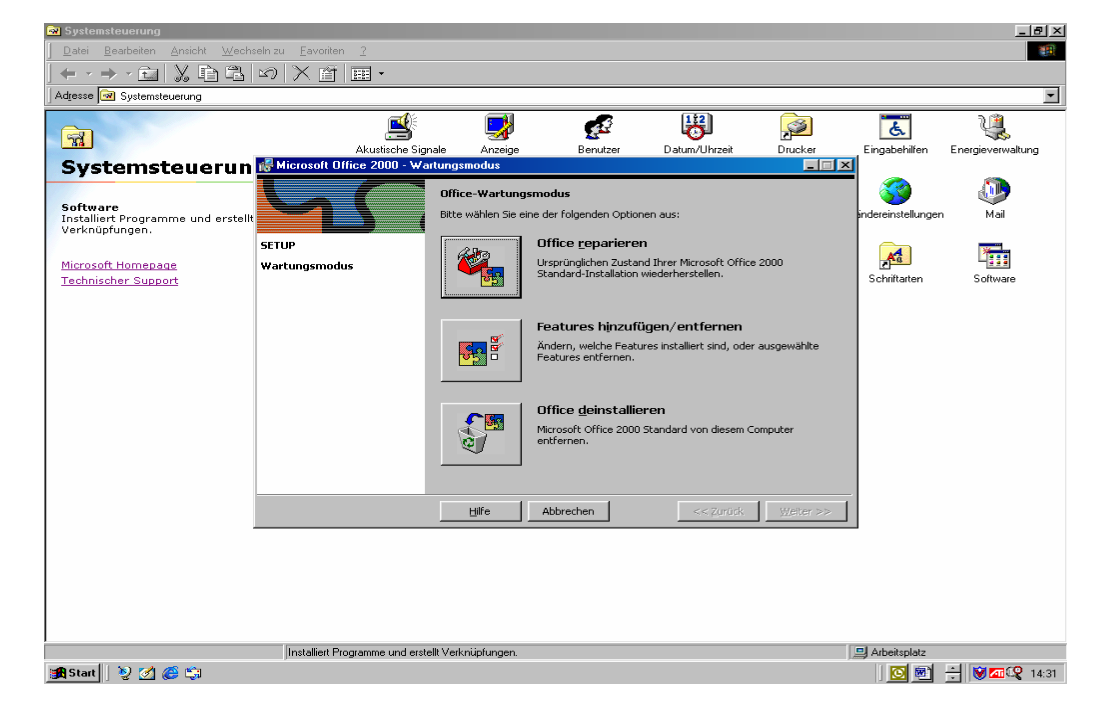
Schritt 3

Nun geht ein weiteres Fenster auf. Markieren Sie das Officepaket und klicken Sie dann auf **>Hinzufügen/Entfernen<**.



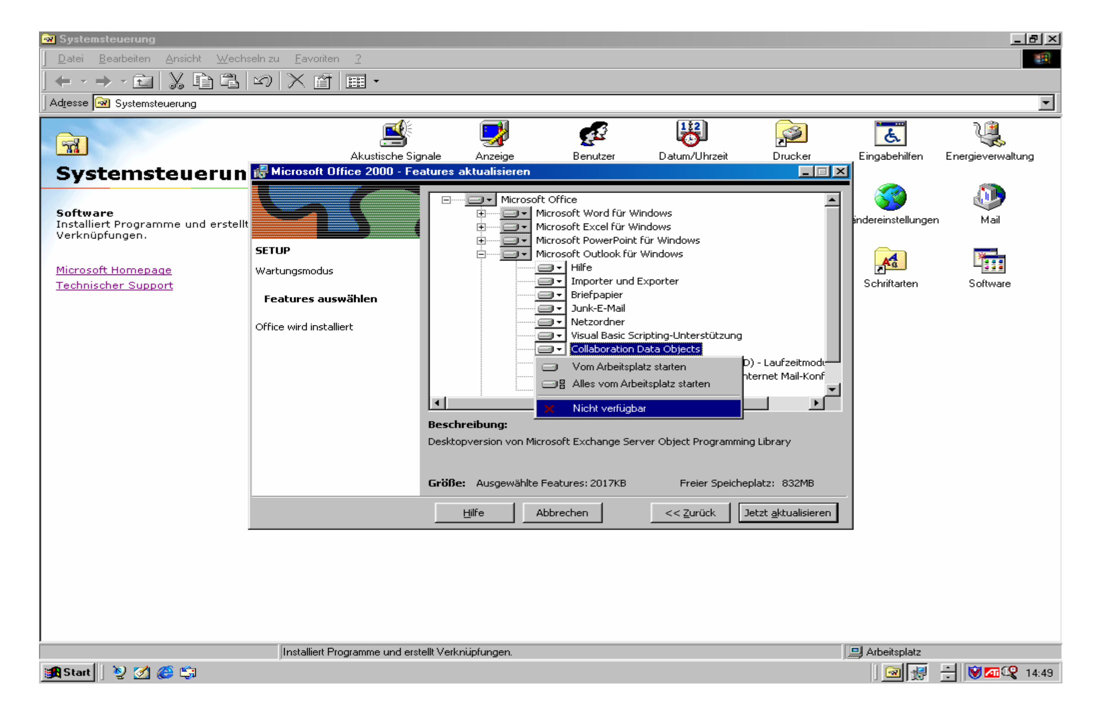
Schritt 4

Jetzt startet das Setup-Programm des Officepaketes. Hier muss **>Features hinzufügen/entfernen<** gewählt werden.

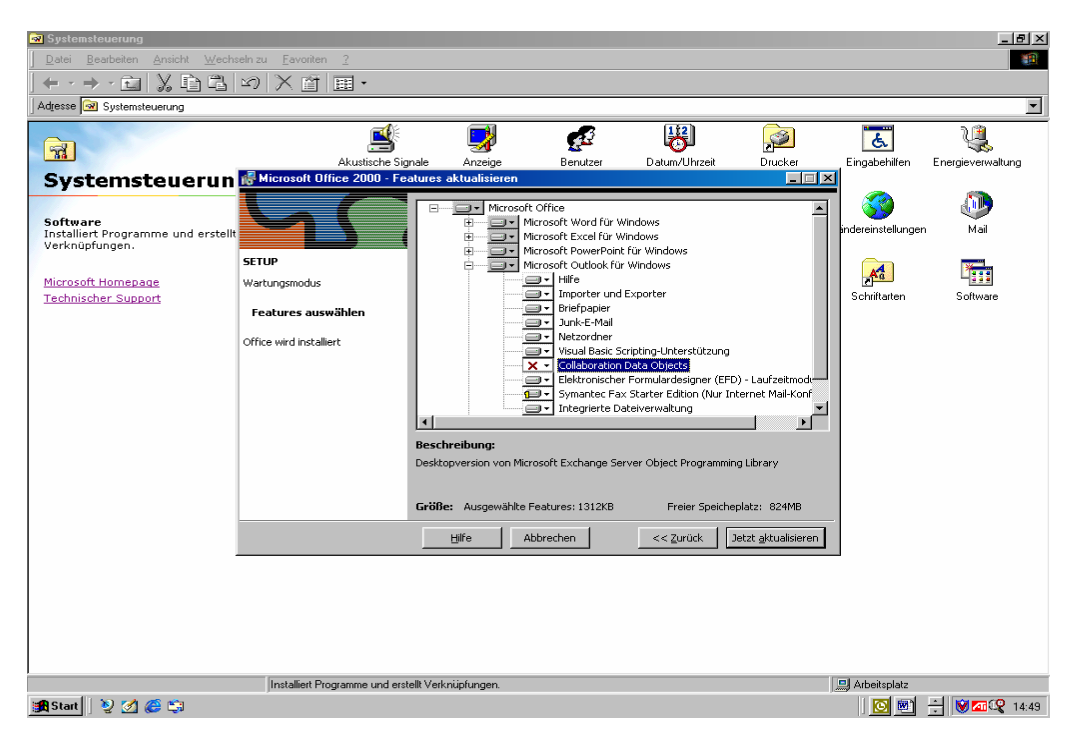


Schritt 5

Öffnen Sie im Menü das Verzeichnis **>Microsoft Outlook für Windows<** und stellen Sie anschließend bei **>Colloboration Data Objects<** auf **>Nicht verfügbar<** um. (Falls die Einstellung schon vorhanden ist, bitte bei Schritt 7 fortfahren.)



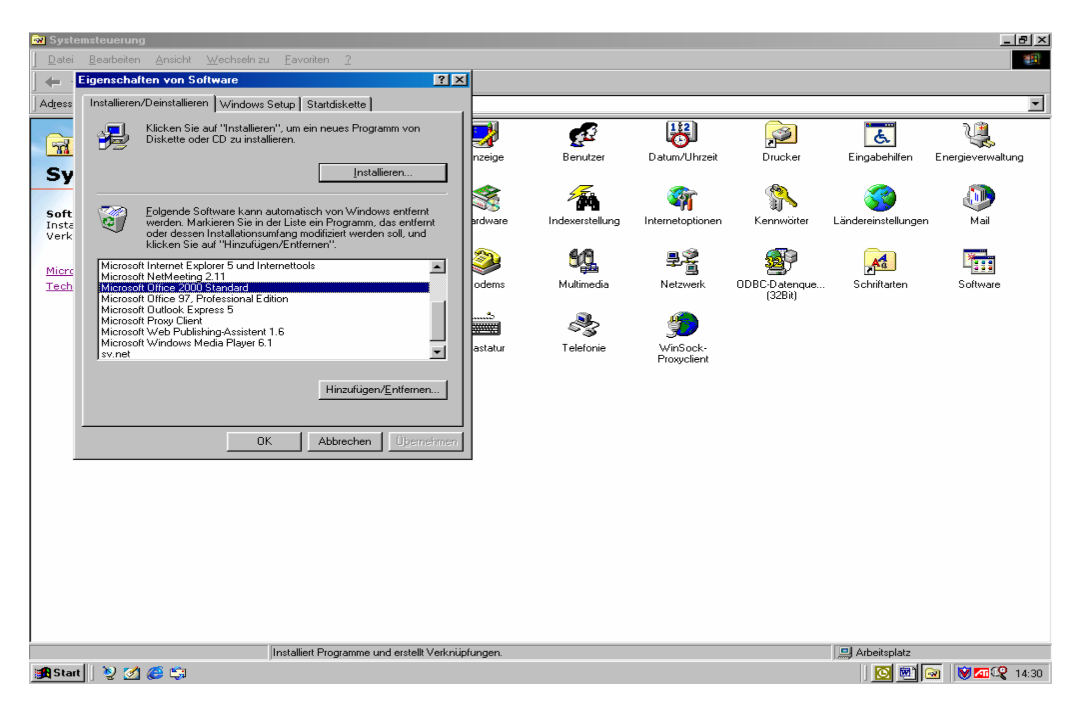
Nachdem auf **>Nicht verfügbar<** umgestellt wurde, klicken Sie nun auf **>Jetzt aktualisieren<** und das Setup wird beendet.



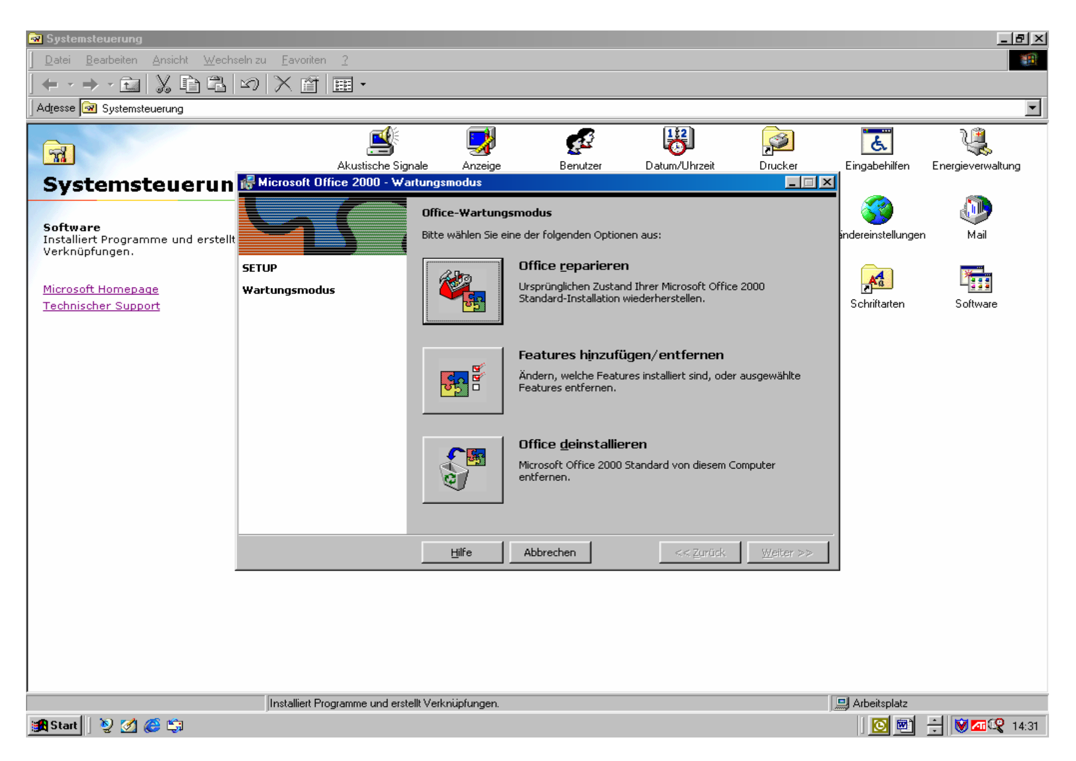
!!! BITTE STARTEN SIE DAS SYSTEM NUN NEU !!!

Schritt 6

Nach einem Systemneustart gehen Sie bitte wieder auf **>Start<**, anschließend auf **>Systemsteuerung<** und dann auf **>Software<**. Hier muss man erneut das Officepaket markieren. Nachdem das geschehen ist, klickt man wieder auf **>Hinzufügen/Entfernen<**.



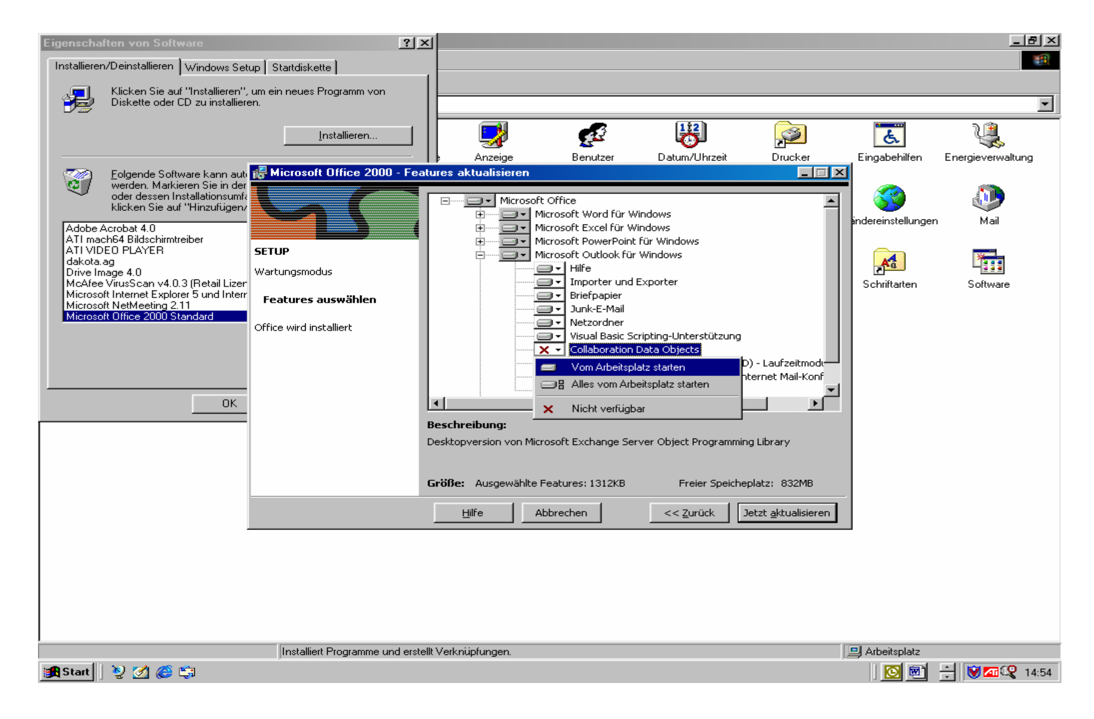
Jetzt startet das Setup-Programm vom Officepaket. In dem nun geöffneten Fenster muss **>Features hinzufügen/entfernen<** gewählt werden.





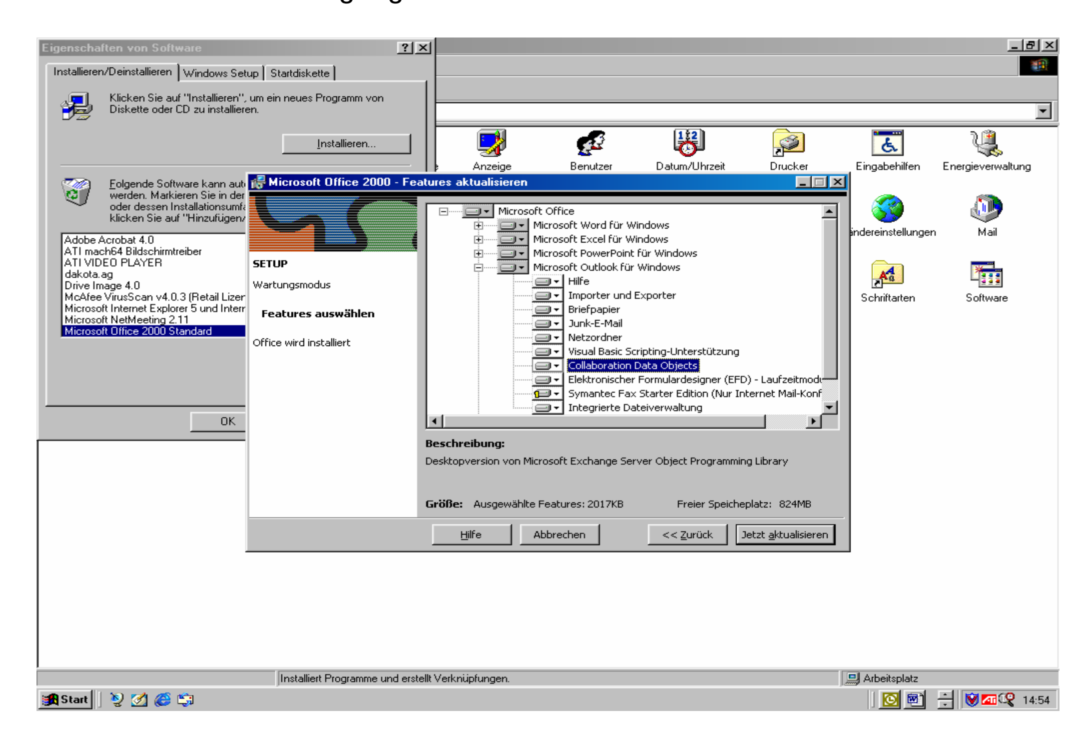
Schritt 7

An diesem Punkt stellt man **>Collaboratio Data Objectes<** auf **>Vom Arbeitsplatz starten<** um.



Schritt 8

Zum Schluss muss der Button **>Jetzt aktualisieren<** angeklickt werden. Die Einstellung wird aktualisiert und der Vorgang ist beendet.



!!! BITTE STARTEN SIE DAS SYSTEM NUN NEU !!!

In Outlook unter **>Extras-Optionen<** bei **>E-Mail-Format<** darauf achten, dass „Nur-Text“ eingestellt ist.



2.5 *Welche Rechte benötige ich bei NT, Windows 2000 oder XP?*

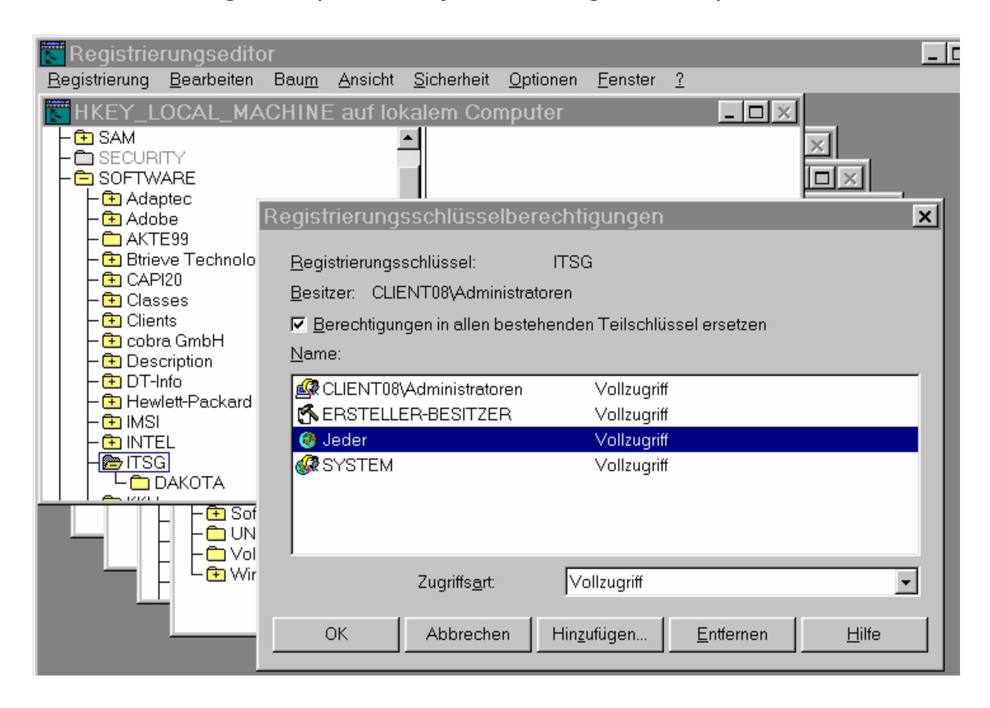
Für die Installation sind Administrator-Rechte notwendig. Sehen Sie dazu im Handbuch nach und sprechen ggf. mit Ihrem Softwarehaus.

Hier finden Sie das dakota-Handbuch zum Download:
http://www.itsg.de/dakotaag/dakota_forum/dateien/Dakota%20Benutzer%20HandbuchV3.0.PDF

Bitte beachten Sie:
Wenn Ihr Arbeitsplatz Mitglied einer Domäne ist, setzen Sie sich bitte mit Ihrem Netzwerkadministrator in Verbindung und führen Sie die Installation als Domain-Administrator aus und nicht als lokaler Administrator.

Um dakota Version 2.8 auch ohne Administratorrechte nutzen zu können, müssen Sie die folgenden Schritte noch durchführen. Ab der Produktversion 3.0 wird dies automatisch durchgeführt.

Bei Windows NT, 2000 oder XP müssen besondere Rechte durch den Administrator vergeben werden. Der NT-Adminstrator muss den Schlüssel HKEY_LOCAL_MACHINE\Software\ITSG für **>Jeder<** auf **>Vollzugriff<** nach der Installation freigeben (WINNT\system32\regedt32, ...).



Den Schlüssel HKEY_LOCAL_MACHINE\Software\ITSG, **>Vollzugriff für Jeder<**, **>Berechtigungen in allen bestehenden Teilschlüssel ersetzen<** anklicken.
Bei Unklarheiten fragen Sie Ihren NT-Systemadministrator.

Bitte kontrollieren Sie Ihre Sicherheitseinstellungen Ihrer Verzeichnisse von dakota, z. B. **C:\dakotaag** und **C:\Programme\dakotaag** und vergeben Sie über „Eigenschaften" -> „Sicherheiteinstellungen" **>Jeder< >Vollzugriff<** und entfernen die vererbaren Berechtigungen.

2.6 *Wie verarbeite ich das Schlüsselverzeichnis Annahme.agv/.key?*

Vom TrustCenter erhalten Sie eine E-Mail mit einem Anhang. Speichern Sie die Datei in das Verzeichnis von dakota (z. B. c:\dakotaag).
Nach dem Speichern verarbeiten Sie die Datei mit einem Doppelklick. **dakota muss dabei geschlossen sein**!

Alternativ können Sie die jeweilige Schlüsseldatei mit dem Assistenten in dakota bearbeiten:
Assistent -> Zertifikate einlesen -> Annahme.* auswählen

oder ab der Produktversion 3.0

Stammdaten -> Stammdatenupdate -> Durchsuchen oder **Über das Internet herunterladen**

Gerne könne Sie die Datei auch online erhalten:

Um die aktuellen Schlüssel der Annahmestellen für das Arbeitgeberverfahren zu erhalten:
http://www.itsg.de/tc/tc/tc-ftp/tc-download/sv.agv.asp

Um die aktuellen Schlüssel der Annahmestellen für das Leistungserbringerverfahren zu erhalten:
http://www.itsg.de/tc/tc/tc-ftp/tc-download/sv.lev.asp

Die ITSG bietet ebenfalls einen Update-Service an. Sollten sich die Schlüssel der Annahmestellen im Gesundheitswesen ändern, erhalten Sie automatisch eine E-Mail:
http://www.itsg.de/tc/service/updateservice.asp

2.7 *Wie sichere bzw. rücksichere ich mein Zertifikat?*

Wenn Sie Ihre Zertifizierungsanfrage an unser TrustCenter bzw. die Zertifizierungsantwort von unserem TrustCenter erhalten haben, d.h. die Betriebsnummer.crp und die annahme.key oder annahme.agv in Dakota eingelesen haben, wird automatisch eine Datensicherung Ihres Zertifikates angelegt.
Die Sicherung befindet sich entweder unter Ihrem Windows-Systemverzeichnis in dem Unterverzeichnis Dakota_S oder Dakota_le oder unter Ihren Eigenen Dateien im Unterverzeichnis Dakota_S oder Dakota_le.

Ab der Produktversion 3.0 von dakota können Sie über den Menüpunkt
Extras -> Sicherung -> Sicherung erstellen jederzeit eine Sicherung anfertigen bzw. über den Menüpunkt **Extras -> Sicherung -> Sicherung importieren** jederzeit eine Sicherung importieren.

Für eine Rücksicherung wenden Sie sich bitte an Ihr Softwarehaus. Der Sicherungsordner enthält alle Daten, die Sie für eine Rücksicherung Ihres Schlüssel benötigen.

Sichern Sie diesen Ordner bitte komplett auf ein externes Medium, z. B. USB-Stick, externe Festplatte, Diskette oder CD, da Ihnen bei Verlust Ihres Zertifikates nur eine Neuzertifizierung bleibt, die Kosten verursacht.

Für eine Rücksicherung wenden Sie sich bitte an Ihr Softwarehaus. Der Sicherungsordner enthält alle Daten, die Sie für eine Rücksicherung Ihres Schlüssel benötigen.

2.8 *Ich habe mein Passwort in dakota vergessen, was muss ich tun?*

Da mit personenbezogenen, sensiblen Daten gearbeitet wird, wurde von Ihnen ein Passwort eingerichtet, als Sie Ihre Schlüsseldatei erzeugt haben.
Das Passwort ist Teil Ihres Zertifikates. Wenn Sie ein Zertifikat beantragen, geben Sie Ihr gewünschtes Passwort ein, dieses wird von Ihnen frei gewählt.

Das Passwort ist Teil Ihres Zertifikates. Wenn Sie ein Zertifikat beantragen geben Sie Ihr gewünschtes Passwort selbst ein, dieses wird von Ihnen frei gewählt und nach einer Zertifizierung auch nicht mehr geändert werden, da Ihr Kennwort fester Bestandteil des Zertifikates ist.

Dieses Passwort können wir leider nicht wiederherstellen, da es verschlüsselt in dakota eingearbeitet wird. Evtl. hat Ihr Softwarehaus, wo Sie Ihr dakota erworben haben, Sie bei der Einrichtung unterstützt und kann Ihnen weiterhelfen.

Sollten Sie Ihr Passwort nicht mehr auffinden können, müssen Sie neu zertifizieren, wodurch Ihnen die Kosten für eine Zertifizierung entstehen. Den aktuellen Zertifikatspreis finden Sie hier: http://trustcenter.itsg.de

2.9 *Wie bzw. wann verlängere ich meinen Schlüssel in dakota?*

Das Zertifikat hat eine begrenzte Laufzeit von drei Jahren. dakota warnt Sie vor dem Ablauf dieses Zeitraumes (z. B. 90 Tage vor Ablauf). Nach diesem Ablauf-Hinweis bearbeiten Sie Ihre Monatsmeldungen noch wie gewohnt und beantragen DANACH einen neuen Schlüssel.

Der dakota-Assistent führt Sie durch die einzelnen Schritte:

Beachten Sie auch:
>1.2 *Wie lange dauert es, bis ich meine Antwort vom TrustCenter erhalte?*<

2.10 *Fehlermeldung ITSG005 (Die Nutzdatendatei entspricht nicht der Namenskonvention (z. B. BWNACxxx ,DUEVMxxx oder EDUA0xxx)*

Die Dateinamen der zu verarbeitenden Dateien entsprechen nicht den Vorgaben. Zulässige Dateinamen finden Sie im technischen Handbuch von dakota im Kapitel „Verschlüsseln“.

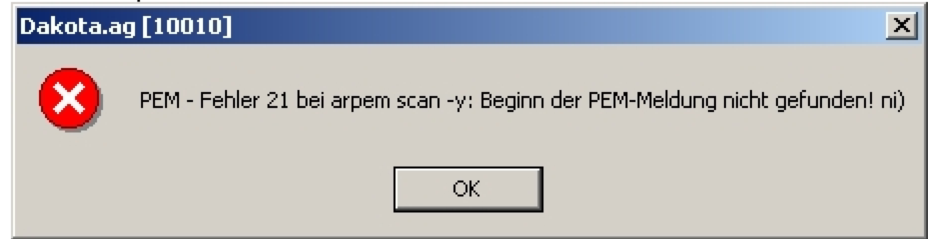
2.11 *Fehlermeldung ITSG016 Fehler beim Prüfen des Vorlaufsatzes*

Der Vorlaufsatz der Melde- oder Beitragsnachweis-Datei konnte nicht gefunden werden. Das Format der Datei ist fest definiert, sehen Sie hierzu die technischen Vorgaben.



2.12 *Ich erhalte den Fehler PEM 21 wenn ich die Zertifizierungsantwort vom TrustCenter einlesen möchte.*

Zum Beispiel:



Beim Empfangen der Zertifizierungsantwort per E-Mail wurde die Zertifikatsdatei (Ihre Betriebsnummer.CRP bzw. Ihre IK-Nummer.CRP) zerstört. Dies liegt im Regelfall an Ihrem eingesetzten E-Mail-Programm, Virenscanner oder Firewall-System.

Bitte entpacken Sie das angehängte Zip-Archiv und versuchen Sie es damit erneut.

Wenn Sie weiterhin diesen Fehler erhalten, können Sie unter http://trustcenter.itsg.de im Bereich Online Auftragsverfolgung die Dateien mit Ihrer Betriebs– und Auftragsnummer erneut herunterladen."



2.13 *Fehlermeldung PEM 22 Ende der PEM-Meldung nicht gefunden*

Siehe „2.12Ich erhalte den Fehler PEM 21 wenn ich die Zertifizierungsantwort vom TrustCenter einlesen möchte.“

2.14 *Fehlermeldung PEM 23 unbekannter Header (kein PEM-Standard)*

Siehe „2.12Ich erhalte den Fehler PEM 21 wenn ich die Zertifizierungsantwort vom TrustCenter einlesen möchte.“



2.15 *Ich erhalte den Fehler PEM 26 wenn ich Daten an die Krankenkasse versenden möchte.*

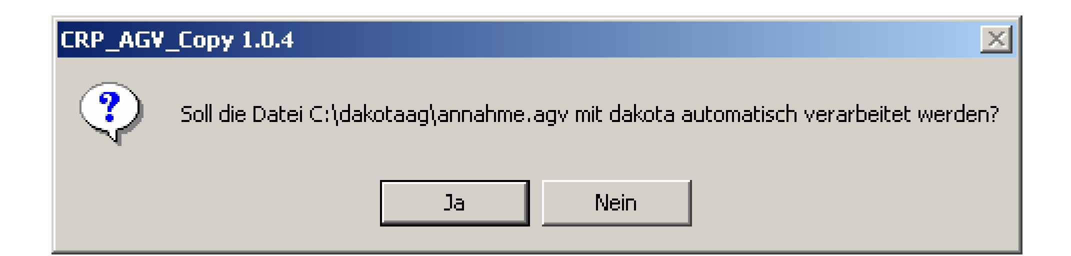
Die Zertifikate der Datenannahmestellen wurden am 01.01.2005 erneuert. Bitte lesen Sie die Datei **Annahme.agv** (für Arbeitgeber) bzw. die Datei **Annahme.key** (für Leistungserbringer) ein. Beachten Sie hierzu die folgenden Schritte, die anhand des Beispiels für die Datei **Annahme.agv** dargestellt sind:

Laden Sie die Datei unter dem folgenden Link auf Ihren PC:
Arbeitgeberverfahren
http://www.itsg.de/tc/tc/tc-ftp/tc-download/cci-ftp-upload/ag/annahme.agv

sonstige Leistungserbringer
http://www.itsg.de/tc/tc/tc-ftp/tc-download/cci-ftp-upload/ag/annahme.key

Schließen Sie das dakota-Programm.

Klicken Sie die Datei **Annahme.agv** bzw. **Annahme.key** doppelt an und bestätigen Sie die folgende Sicherungsrückfrage mit **>JA<**.

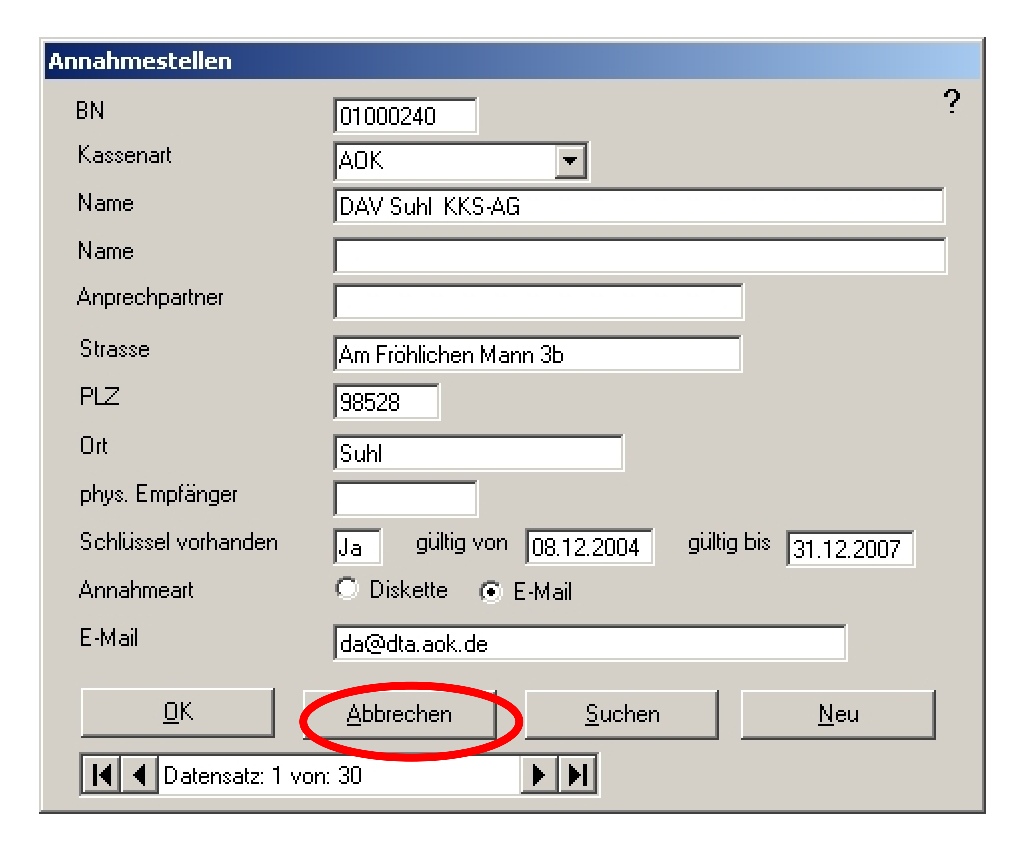


Beim Einlesen der **Annahme.agv** bzw. **Annahme.key** kommt die folgende Meldung:



Bitte ignorieren Sie diese Meldung. Es handelt sich hierbei lediglich um eine neue Annahmestelle im Gesundheitswesen. Der Verband der Deutschen Rentner (VDR) wurde für ein spezielles Datenaustauschverfahren aufgenommen. Für Sie als Arbeitgeber hat dieses Verfahren keine Bedeutung.

Bestätigen Sie die Meldung mit >OK< und verlassen Sie die nächste Maske einfach mit >Abbrechen<.



Die gleichen Schritte befolgen Sie bitte, wenn Sie sich die Datei **Annahme.key** runterladen möchten.

Anschließend können Sie Ihre Daten wieder verschlüsseln und versenden.

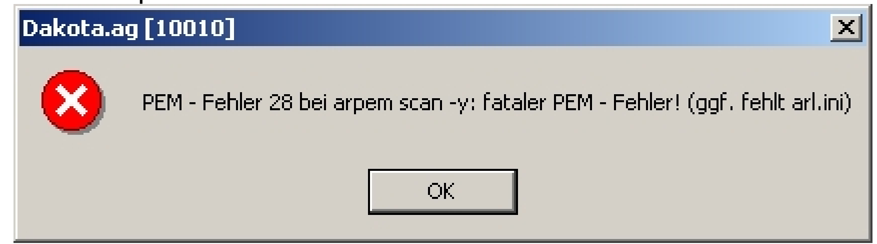
Beachten Sie bitte, dass Sie zunächst alle fehlerhaften Dateien über das >Kurzprotokoll< löschen, bevor Sie weitere Dateien mit dakota versenden können.

Ab der dakota Produktversion 3.0 führen Sie bitte das Stammdaten-Update von dakota aus.



2.16 *Ich erhalte den Fehler PEM 28 wenn ich die Zertifizierungsantwort vom TrustCenter einlesen möchte.*

Zum Beispiel:



Diese Problem kann mehrere Ursachen haben:

Zertifizierungsantwort wurde beschädigt

Ihre Zertifizierungsantwort wurde beschädigt, bitte führen Sie die Schritte des folgenden Kapitels aus**: 2.12 Ich erhalte den Fehler PEM 21 wenn ich die Zertifizierungsantwort vom TrustCenter einlesen möchte.**

Es befindet sich eine Online-Banking-Software der Deutschen Bank auf dem PC.

Beide Produkte stören sich gegenseitig auf dem PC. Bitte deinstallieren Sie die Applikation von Ihrem PC und entfernen Sie zusätzlich den Registrykey **HKEY_CURRENT_USER\Software\ARL** manuell. Nach einem Neustart des Rechners funktioniert dakota wieder.

Das Zertifikat passt nicht mehr zu Ihrem privaten Schlüssel.

In diesem Falle haben Sie, nachdem Sie die Anfrage an das TrustCenter gesendet haben, einen neuen Schlüssel erzeugt. Durch diese Fehlbedienung ist Ihr Zertifikat unbrauchbar geworden und kann nicht verwendet werden. Es gibt keine andere Lösung, als einen neuen Antrag an das TrustCenter zu senden.

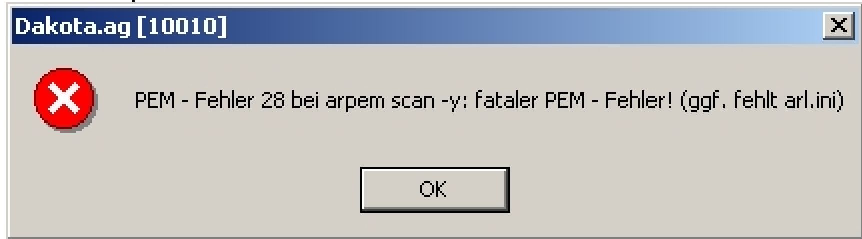
Ab der Produktversion 3.0 liegt Ihnen sicherlich eine Sicherung Ihrer Zertifikatsanforderung an das ITSG TrustCenter vor. Sehen Sie hierzu: 2.7 Wie sichere bzw. rücksichere ich mein Zertifikat?

WICHTIGER HINWEIS: JEDER ZERTIFIZIERUNGSANTRAG IST EIN SCHRIFTLICHER AUFTRAG UND WIRD MIT DER AKTUELLEN GEBÜHR FÜR EIN ZERTIFIKAT BERECHNET!!!!

Für Details sehen Sie bitte: **Fehler! Verweisquelle konnte nicht gefunden werden. Fehler! Verweisquelle konnte nicht gefunden werden.**

2.17 *Ich erhalte den Fehler PEM 28 wenn ich dakota starte.*

Zum Beispiel:



Dieses Problem kann mehrere Ursachen haben:

dakota wurde in ein Netzlaufwerk installiert.

Bitte deinstallieren Sie dakota und installieren Sie die Software erneut. Bitte achten Sie bei der Neuinstallation darauf, dass Sie ausschließlich auf einem lokalen Datenträger installieren.

Es befindet sich eine Online-Banking-Software der Deutschen Bank auf dem PC.

Beide Produkte stören sich gegenseitig auf dem PC. Bitte deinstallieren Sie die Applikation von Ihrem PC und entfernen Sie zusätzlich den Registrykey **HKEY_CURRENT_USER\Software\ARL** manuell. Nach einem Neustart des Rechners funktioniert dakota wieder.

Das Zertifikat passt nicht mehr zu Ihrem privaten Schlüssel

Es wurde nachdem ein Antrag an das TrustCenter gesendet wurde, wieder ein neuer Schlüssel erzeugt, d. h. Sie haben Ihren privaten Schlüssel überschrieben. Hierfür gibt es keine Lösung außer dakota neu zu installieren. Die Kostensituation ist in den AGB´s des TrustCenters dokumentiert.

WICHTIGER HINWEIS: JEDER ZERTIFIZIERUNGSANTRAG IST EIN SCHRIFTLICHER AUFTRAG UND WIRD MIT DER AKTUELLEN GEBÜHR FÜR EIN ZERTIFIKAT BERECHNET!!!!

2.18 *Ich erhalte den Fehler PEM 28 wenn ich einen Schlüssel in dakota generiere.*

Zum Beispiel:
PEM – Fehler 28 bei **arp_unlock_user**: fataler PEM –Fehler! (ggf. fehlt arl.ini)



Testversion

In diesem Fall haben Sie die Testversion von dakota installiert. In der Testversion können Sie nur die Betriebs– bzw. IK-Nummer 12345678 bzw. 123456789 verwenden.

Sollten Sie diese dakota Version für den Produktivbetrieb mit Ihrer echten Betriebs– bzw. IK-Nummer benötigen, wenden Sie sich bitte an Ihr Softwarehaus, von dem Sie dakota erworben haben, um eine Vollversion zu erhalten.

Es befindet sich eine Online-Banking-Software der Deutschen Bank auf dem PC.

Beide Produkte stören sich gegenseitig auf dem PC. Bitte deinstallieren Sie die Applikation von Ihrem PC und entfernen Sie zusätzlich den Registrykey **HKEY_CURRENT_USER\Software\ARL** manuell. Nach einem Neustart des Rechners funktioniert dakota wieder.

2.19 *Fehlermeldung PEM 30 Der Empfänger-Alias konnte nicht aufgelöst werden.*

Diese Fehlermeldung kann beim Verschlüsseln auftreten und bedeutet, dass versucht wird eine Datei an eine Annahmestelle zu senden, die in dakota nicht bekannt ist. Man muss überprüfen, ob die Betriebsnummer bzw. IK-Nummer der Annahmestelle korrekt ist und ob bei dakota in den Annahmestellen das Zertifikat der Annahmestelle korrekt vorhanden ist, d.h., ob die Laufzeit des Zertifikats noch gültig ist.

Um sicher zu stellen, dass Ihr dakota über alle aktuellen Annahmestellen im deutschen Gesundheitswesen verfügt, können Sie sich ein Stammdaten-Update für dakota Version 2.8 herunterladen:

http://www.itsg.de/produkte/produkte.dakota.updatepatch.asp

Sollte Ihr Problem dadurch nicht gelöst werden können, führen Sie bitte noch die Schritte unter folgendem Punkt aus:

Ich erhalte den Fehler PEM 26 wenn ich Daten an die Krankenkasse versenden möchte.

Ab der Produktversion 3.0 führen Sie bitte das Stammdaten-Update von dakota aus.

2.20 *Die Zertifizierungsantwort vom TrustCenter lässt sich nicht einlesen und das Zip-Archiv scheint auch beschädigt zu sein. Was muss ich tun?*

In diesem Fall ist Ihre Antwort vom TrustCenter unterwegs von einem Virenscanner verändert bzw. beschädigt worden.

Sobald Sie die schriftlichen Antragsunterlagen beim ITSG einsenden und diese erfasst wurden, erhalten Sie von uns eine Auftragsnummer per E-Mail.

Nach Erhalt Ihrer Auftragsnummer können Sie den Stand Ihres Antrages jederzeit im Internet unter http://trustcenter.itsg.de im Bereich Online Auftragsverfolgung einsehen und sich Ihre Zertifizierungsantwort erneut herunterladen.



2.21 *Nachdem ich die Zertifizierungsantwort vom TrustCenter und die annahme.agv bzw. annahme.key in Dakota eingelesen habe, bleibt der 2.Schritt im dakota-Assistenten immer offen*

1. Vom TrustCenter erhalten Sie eine E-Mail mit Anhängen. Speichern Sie die Dateien in das Verzeichnis von dakota (z. B. c:\dakotaag).
Nach dem Speichern verarbeiten Sie die Datei mit einem Doppelklick. **dakota muss dabei geschlossen sein**!

Bei geöffnetem Dakota:
Alternativ können Sie die jeweilige Schlüsseldatei mit dem Assistenten in dakota bearbeiten.

2. Stellen Sie sicher, dass Sie die aktuelle annahme.agv bzw. annahme.key besitzen und versuchen Sie es hiermit erneut.

Um die aktuellen Schlüssel der Annahmestellen für das Arbeitgeberverfahren zu erhalten:
http://www.itsg.de/tc/tc/tc-ftp/tc-download/sv.agv.asp

Um die aktuellen Schlüssel der Annahmestellen für das Leistungserbringerverfahren zu erhalten:
http://www.itsg.de/tc/tc/tc-ftp/tc-download/sv.lev.asp

Die ITSG bietet ebenfalls einen Update-Service an. Sollten sich die Schlüssel der Annahmestellen im Gesundheitswesen ändern, erhalten Sie automatisch eine E-Mail:
http://www.itsg.de/tc/service/updateservice.asp

Ab der Produktversion 3.0 führen Sie bitte das Stammdatenupdate von dakota aus.

3. Schließen Sie dakota, löschen Sie in Ihrem Dakota-Verzeichnis (z. B. C:\Dakotaag) die Dateien „imported.ca“ und „cadbs.txt“ und lesen die Zertifizierungsantwort wie unter Punkt 1 beschrieben erneut ein.

4. Bitte überprüfen Sie Ihre Berechtigungen UND den Schreibschutz in Ihrem dakota-Verzeichniss (z. B. C:\Dakotaag und C:\Programme\Dakotaag] und die Windows-Registrierung (mit regedt32: HKEY_LOCAL_MACHINE\SOFTWARE\ITSG) und setzen diese auf „Jeder“ „Vollzugriff“ und entfernen den Schreibschutz auch für die Unterordner bei allen Verzeichnissen
In der Regel treten Berechtigungsprobleme nur auf, wenn Sie nicht über Administratorrechte verfügen .
Im Anschluss lesen Sie die Zertifizierungsantwort wie unter Punkt 1 beschrieben erneut ein.

5. Bitte überprüfen Sie, ob Sie eine Testversion bzw. Demo mf.dat im Einsatz haben. Schließen Sie dakota und ersetzen Sie die Datei mf.dat entweder unter C:\Programme\dakotaag\DLL bzw. C:\dakotaag\System.
Ihr Softwarehaus wird Ihnen hierbei gerne behilflich sein.



2.22 *Fehlermeldung: 3051 in der Funktion bSetTrust*

... The Microsoft Jet database engine cannot open the file c:\Programme\dakotaag\dakota20.mdb. It is already opened exclusively by another user, or you need permission to view its data.

Dieses Problem tritt häufig nach dem Rückspielen der Sicherung auf und kann mehrere Ursachen haben:

Bitte entfernen Sie den Schreibschutz von dakota20.mdb.

Klicken Sie hierfür mit der rechten Maustaste auf die ungeöffnete Datei und klicken Sie dann mit der linken Maustaste auf **>Eigenschaften<**. Wenn in der nun geöffneten Maske bei >**Schreibgeschützt<** ein Häkchen gesetzt ist, entfernen Sie es bitte.

Überprüfen Sie Ihre Berechtigungen.

Die Datei dakota20.mdb können Sie beispielsweise unter: C:\Programme\dakotaag\dakota20.mdb finden.

Eventuell ist noch die Datenbank geöffnet. Bitte schließen Sie diese.

Dakota20.mdb ist eine Access 97-Datenbank. Diese auf keinen Fall mit Access 2000, XP und 2003 konvertieren.

2.23 *Fehler 429 beim Öffnen einer E-Mail-Sitzung am E-Mail-Standardprogramm "Microsoft Outlook"! ActiveX component can't create object*

Diese Fehlermeldung tritt ab der Produktversion 3.0 entweder im Assistenten beim Versenden der Test-E-Mail oder beim „Daten verarbeiten“ auf.

In diesem Fall ist die CDO-Schnittestelle von Outlook nicht korrekt installiert. Bitte führen Sie die Punkte unter **2.4 Das Versenden mit Outlook 2000/2002/2003 funktioniert nicht?** aus.

2.24 *Fehler 713 (Anwendungs- oder objektdefinierter Fehler) in der Assistent.exe*

In dieser Fehler tritt beim Drucken der Unterlagen bzw. des Zertifizierungsantrages auf. Diese Konstellation kann mehrere Ursachen haben:

1. Ihr System wurde nach der dakota-Installation nicht neugestartet. Bitte versuchen Sie es nach einem Neustart erneut.

2. Auf Ihrem System konnte die DLL actrpt.dll nicht registriert werden. Bitte über **Start** -> **Ausführen** -> **regsvr32 actrpt.dll** die actrpt.dll registrieren.

2.25 *SMTP-Fehler -1 Die Verbindung zum Server konnte nicht hergestellt werden oder Fehler beim Schreiben auf den Socket.*

Das Problem kann mehrere Ursachen haben. Bitte kontrollieren Sie folgenden Angaben:

- ist der Name bzw. IP-Adresse des SMTP Server korrekt

- Bitte kontrollieren Sie, dass die Verbindung nicht blockiert wird, z. B. Windows-Firewall, anderes Firewall-Produkt, Virenscanner, etc.
  Auch ein deaktivierter Virenscanner kann blockieren.

  Bitte fügen Sie bei den Firewall- und Virenscanner-Produkten die **dakota20.exe** bzw. **dakota30.exe** und die **Assistent.exe** bzw. **AssistentLE.exe** als "berechtigtes" oder vertrauenswürdiges Programm hinzu.

Die Fehlermeldung weist auf eine Besonderheit, bei der Systemumgebung des Kunden hin und ist kein Fehler der Software.

Workaround:

Richten Sie dem Kunden ein Postfach bei einem Freemail-Provider ein (z. B. GMX, WEB.DE, etc.) ein und versuchen Sie es hiermit. Ein Vorbelegung der Werte finden Sie in dakota ab der Produktversion 3.0

2.26 *SMTP-Fehler 1 Dateiname der Bodydatei fehlt, Argument nicht OK.*

Das Problem kann mehrere Ursachen haben. Bitte kontrollieren Sie die folgenden Angaben:

- Bitte kontrollieren Sie, dass die Verbindung nicht blockiert wird, z. B. Windows-Firewall, anderes Firewall-Produkt und Virenscanner, etc.
  Auch ein deaktivierter Virenscanner kann blockieren.

  Bitte fügen Sie bei den Firewall- und Virenscanner-Produkten auf jeden Fall die **dakota20.exe** bzw. **dakota30.exe** und die **Assistent.exe** bzw. **AssistentLE.exe** als "berechtigtes" oder vertrauenswürdiges Programm hinzu.
  Beispiele finden Sie in den Kapiteln
  Wie richte ich meine Symantec Produktreihe für dakota ein (z. B. Norton Antivirus 2005, Norton Internet Security 2005, Norton Personal Firwall 2005) ?

- Die Anmeldeinformationen am SMTP-Server scheinen nicht korrekt zu sein.
  Bitte versuchen Sie den SMTP-Versand mit Authentifizierung.
  Die Anmeldeinformationen erhalten Sie von Ihrem E-Mail-Administrator oder von Ihrem Provider.

  Zum Beispiel:
  1. Eigener E-Mail-Server
  In einer Exchange-Umgebung verwenden Sie bitte folgenden Angaben:
  SMTP-Server: Eigener E-Mail-Server
  Port: 25
  Benutzername: Windows-Domäne\Domänen-Benutzer
  Passwort: Windows-Kennwort

  2. Provider T-Online
  Bitte beachten Sie, dass T-Online hier eine Besonderheit aufweist. Bitte kontrollieren Sie, dass Sie auch mit T-Online in das Internet eingewählt sind. T-Online führt seine Authentifizierung direkt über die Einwahl durch

  SMTP-Server: mailto.t-online.de
  Port 25
  Authentifizierung nicht verwenden.

  3. Provider AOL
  Bitte beachten Sie, dass AOL beim SMTP-Versand einen Besonderheit aufweist. Der SMTP-Port ist nicht 25 (Standard), sondern 587.
  Bitte kontrollieren Sie, dass die Verbindung nicht blockiert wird, z. B. Windows-Firewall, Virenscanner, etc.

  SMTP-Server: smtp.de.aol.com
  Benutzername: AOL-Name
  Passwort: AOL-Passwort
  Port 587

Die Fehlermeldung weist auf eine Besonderheit, bei der Systemumgebung des Kunden hin und ist kein Fehler der Software.

2.27 *SMTP-Fehler -5 In der Headerdatei stehen nicht genügend Informationen.*

In diesem Fall ist in Ihren Stammdaten der Annahmestellen keine E-Mail Adresse für die Annahmestelle eingetragen.
Bitte tragen Sie die E-Mail Adresse ein oder führen Sie das Stammdaten-Updaten von dakota aus.

Eine Auflistung der E-Mail Adressen finden Sie im Kapitel > 1.13 Wie finde ich die Daten der Annahmestellen, z. B. die E-Mail-Adressen?

2.28 *Fehler-Nr 3447 (The Jet VBA file (VBAJET.dll for 16-bit versions,or VBAJET32.dll for 32-bit versions) failed to initialize when called. Try reinstalling the application that returned the error.)*

Sie erhalten diese Meldung, wenn Sie versuchen dakota zu starten. In diesem Fall wurden DLLs der DAO 3.51-Runtime Umgebung auf diesem System durch andere Anwendungen ersetzt bzw. deinstalliert.

Lösung:

Sie führen das Setup von dakota erneut über die Funktion „Aktualisierung“ als Administrator durch. Hierbei wird die erforderlich Laufzeitumgebung (DAO 3.51) erneut installiert und versuchen Sie es erneut.

2.29 *Ich erhalten eine Fehlermeldung, wenn ich den Update-Patch für dakota starte. Was soll ich tun?*

Ich erhalte die folgende Fehlermeldung, wenn ich den Update für dakota (UpdatePatch.exe) starte:



In diesem Fall ist auf Ihrem System keine VB Runtime-Umgebung installiert. Bitte führen Sie das dakota Stammdaten-Update manuell durch.

1. Schließen Sie dakota

2. Laden Sie das dakota Stammdaten-Update herunter und speichern Sie dieses auf Ihrer Festplatte Ihres dakota Systems:
http://www.itsg.de/dakotale/dakota_forum/dateien/UpdatePatch.zip

3. In diesem Zip-Archiv finden Sie eine manuelle Update Anleitung als PDF-Datei ab Seite 2

2.30 *Wie richte ich meine Symantec Produktreihe für dakota ein (z. B. Norton Antivirus 2005, Norton Internet Security 2005, Norton Personal Firwall 2005) ?*

Nach unseren Erfahrungen ist Norton Internet Security die bei Kunden am häufigsten eingesetzte Internetschutzlösung. Sie stellt eine Kombination aus einer Firewall und einem Antivirenprogramm dar. Somit sind auch ein Zugangsschutz, ein Mailwurmschutz und ein Spamfilter integriert. Um das Programm zu konfigurieren öffnen Sie es durch einen Doppelklick auf das gelbe Symbol in der Taskleiste. Es stellt sich Ihnen folgendes Bild dar:

Norton Internet Security
Blockieren | LiveUpdate | Optionen | Hilfe und Unterstützung

Norton Internet Security
Status & Einstellungen
Angriffswarnung
Statistik
Abonnementstatus
Benutzerkonten
Norton AntiVirus
Norton AntiSpam

Systemstatus: Achtung dringend

Sicherheit	Aus
Angriffswarnung	Ein
Persönliche Firewall	Deaktiviert
Intrusion Detection	Deaktiviert
Norton AntiVirus	Achtung
Norton AntiSpam	

Einstellungen für: Supervisor

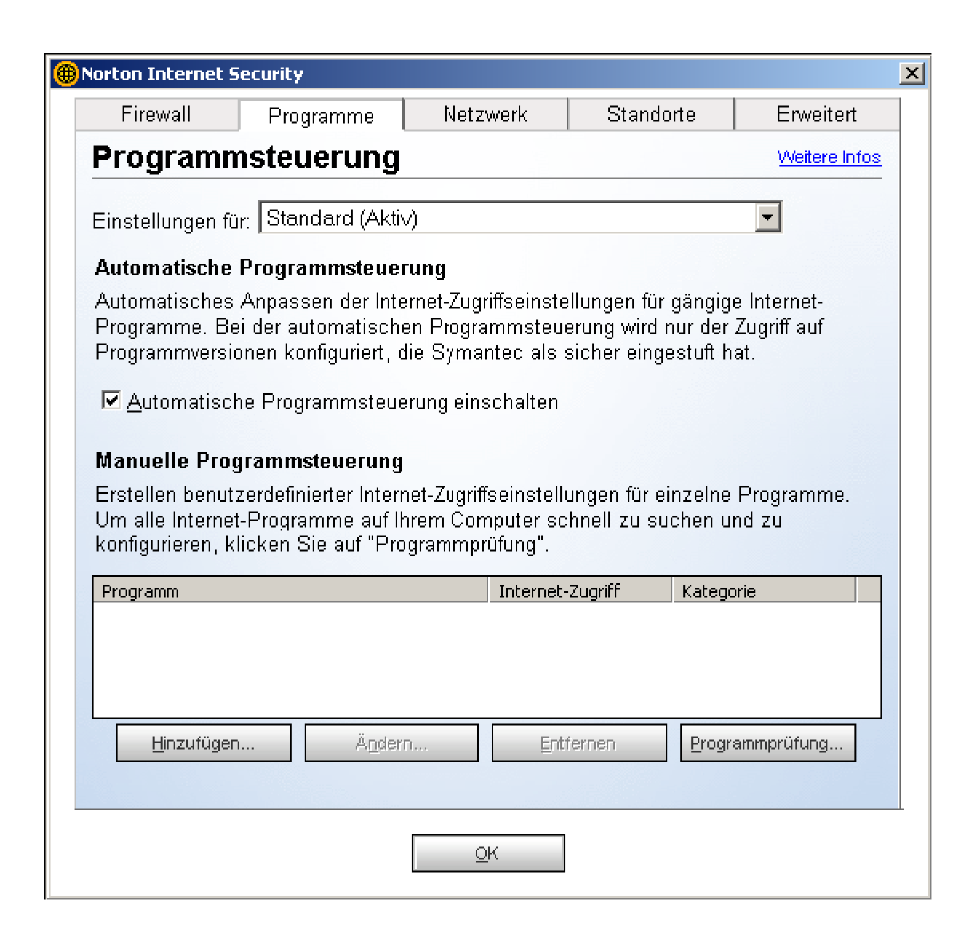
Datenschutz	Deaktiviert
Kindersicherung	Deaktiviert

Persönliche Firewall
Die persönliche Firewall schützt Ihren Computer weitgehend vor unberechtigten Zugriffen.
Weitere Infos
Ausschalten
Konfigurieren

symantec.
Norton Internet Security 2005

Klicken Sie auf „***Persönlicher Firewall***“ und „***Konfigurieren***“. Wählen Sie im folgenden Fenster den Reiter „***Programme***“.

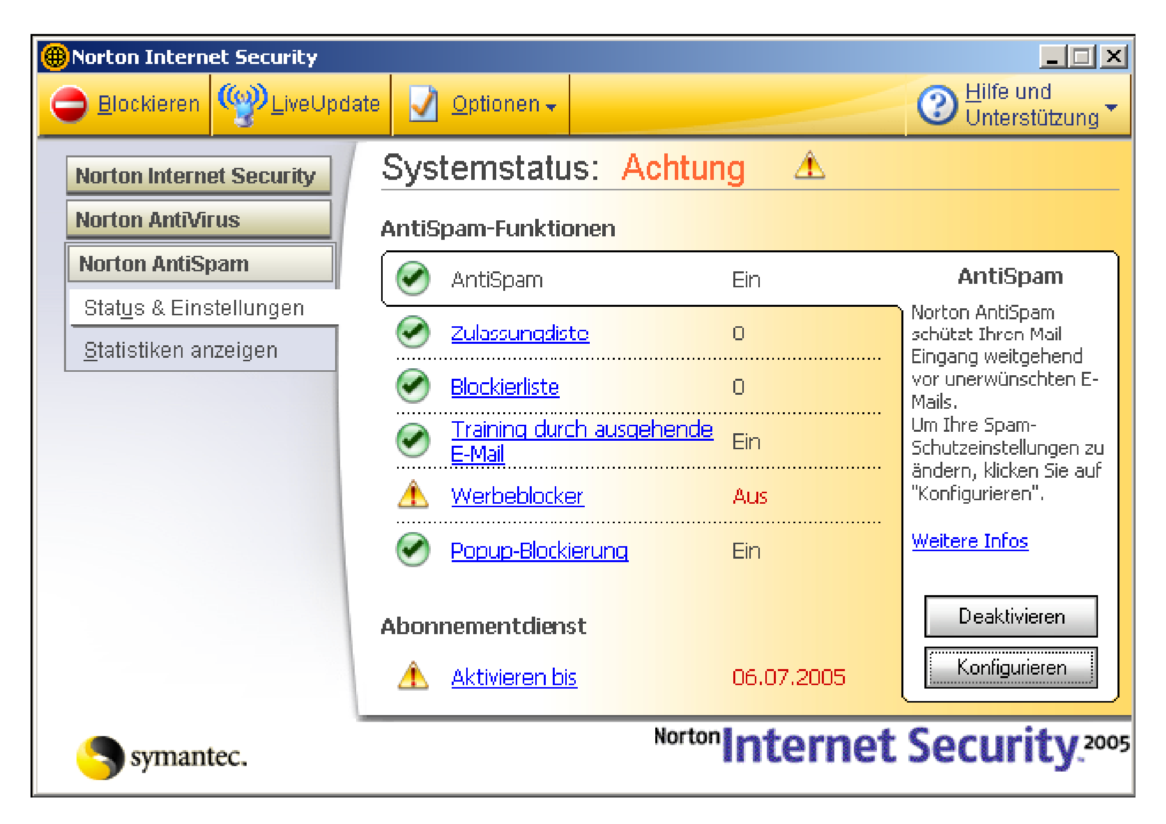
Je nach Konstellation fügen Sie hier bitte „***Dakota20.exe oder Dakota30.exe***“ (C:\Programme\Dakotaxx) ein.
Ab der Produktversion 3.0 fügen Sie bitte noch die Datei **Assistent.exe** oder **AssistentLE.exe** unter (C:\Programme\Dakotaxx) ein.
Während des Hinzufügens können Sie den Status des Programms festlegen. Wählen Sie hier „***Alle Aktionen zulassen***“. Damit ist dakota berechtigt Internetverbindungen zu initialisieren und Daten zu übertragen.



Bestätigen Sie alles mit „OK“.

Wählen Sie unter „Optionen“ Norton Antivirus aus. Im folgenden Fenster wählen Sie links den Punkt „E-Mail“. In der folgenden Konfigurationsmaske entfernen Sie bitte die Hacken: - Ausgehende E-Mails prüfen und
Wurm-Blockierung aktivieren. Zuletzt bleibt die Konfiguration des Spamfilters AntiSpam. Diese ist nur nötig, wenn die Sendung durch das Standard E-Mail-Programm erfolgt. Wird der dakota interne SMTP Client benutzt, ist dies überflüssig.

Öffnen Sie die Konfiguration durch Anwahl des Buttons aus dem linken Menü. und klicken Sie rechts unten auf „Konfigurieren“



Sie gelangen zum folgenden Fenster. Importieren Sie hier das Adressbuch des Standard-E-Mail-Programms.



Ab Norton Antivirus Version 2005 ist ein Spamfilter und eine Mailwurmprotektion integriert. Dadurch ist bei der Installation von dakota und der Konfiguration eines externen Mail-Programms darauf zu achten, dass hier eine Nachkonfiguration erfolgt.

Starten Sie dazu Norton Antivirus mittels des gelben Symbols rechts in der Taskleiste. Und folgen Sie den Anweisungen im Abschnitt Norton Internet Security 2005.

2.31 *Wie richte ich mein Anti-Virus Programm McAfee V9.0 ein?*

Um McAfee zu konfigurieren öffnen Sie das Securitycenter und wählen Sie „*Virusscan*“ auf der linken Seite.

McAfee SecurityCenter

McAfee securitycenter

updates support help

my security center

virusscan professional

personal firewall plus

privacy service

spamkiller

VirusScan is currently protecting your computer from viruses.
Click here if you want to disable VirusScan.

VirusScan Help About VirusScan

I want to...

Scan My Computer for Viruses
Thoroughly scan programs and documents to check your computer for viruses and potentially unwanted programs.

Configure VirusScan Options
Review and modify all of your VirusScan options.

Manage Quarantined Files
Quarantine a program or document when you think it might be infected.

View the World Virus Map
Get a real-time, bird's-eye view of where the latest viruses are infecting computers worldwide.

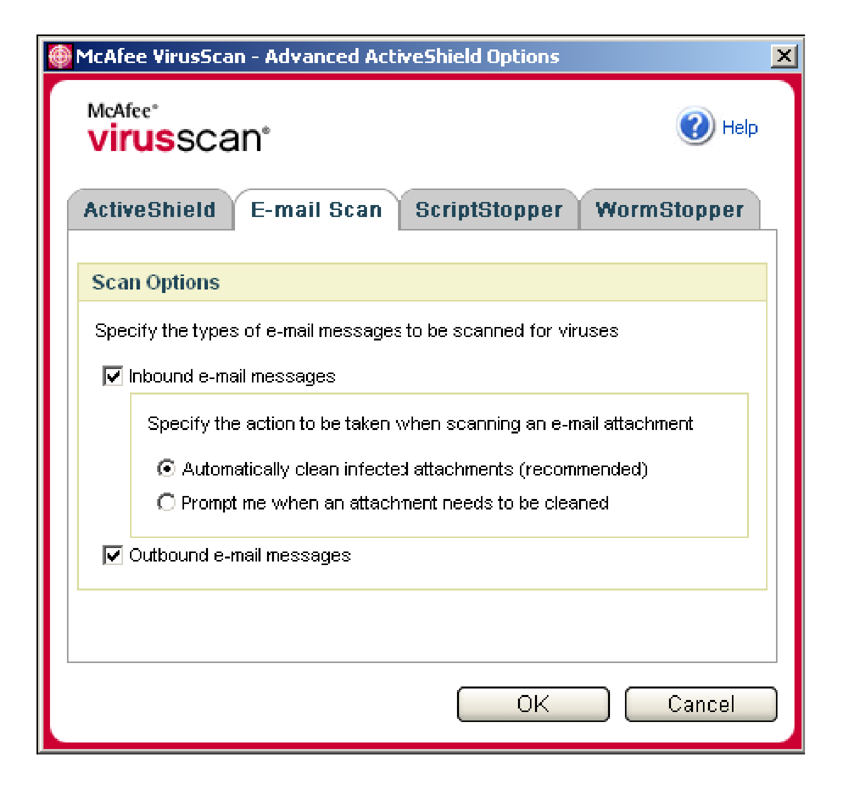
Find Out About Viruses
Is it real or a hoax? Look it up in the definitive computer virus information database.

Create a Rescue Disk
If your computer is infected by a virus and will not start, a Rescue Disk will get your computer up and running.

Wählen Sie die Konfiguration aus und klicken Sie im folgenden Fenster auf „***Erweitert***“. Damit können Sie nicht nur vorgegebene Werte anpassen sondern etwas tiefer in den Schutzmechanismus eingreifen.

Entfernen Sie die Haken um den reibungslosen Datentransfer zu ermöglichen:

Reiter **E-Mail Scan** -> **outbound e-mail messages**



Reiter **WormStopper** -> **Enable Wormstopper** und
-> **Alert me when „5“ emails are sent within 30 seconds**

Nach Durchführung der Änderungen speichern Sie alles mit >OK< und die Konfiguration ist beendet.

